UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 5 | Issue 1 Article 8

2001

Willie Sutton Is on the Internet: Bank Security Strategy in a Shared Risk Environment

Eugene M. Katz

Theodore F. Claypoole

WILLIE SUTTON IS ON THE INTERNET: BANK SECURITY STRATEGY IN A SHARED RISK ENVIRONMENT

EUGENE M. KATZ*
THEODORE F. CLAYPOOLE**

TABLE OF CONTENTS

* Member, Womble Carlyle Sandridge & Rice, PLLC, Charlotte, North Carolina; B.A. 1970; J.D., 1972, Tulane University.
** Of Counsel, Womble Carlyle Sandridge & Rice, PLLC, Charlotte, North Carolina; A.B., 1985, Duke University; J.D., 1988, Ohio State University.

I. INTRODUCTION

A bank's most ancient, basic functions include protection of valuable property and facilitation of commerce. In the early Renaissance, Italian banking families kept money and treasure secure from the risks of the day and provided letters of credit to travelling merchants. As the United States grew into a financial power, the Morgans and the Mellons and the Chases used state-of-the-art security measures to guard the nation's riches and created cutting-edge financial strategies to sate the nation's insatiable hunger for manufactured goods and transportation networks. Now the global economy demands a staggering array of commercial facilitation services from financial service companies: funding the fabrication and information economy, lubricating worldwide hyper-efficient instant-access marketplaces, liberating capital to endow new ideas, and democratizing access to sophisticated instruments. But security demands on these companies have also exploded in size and complexity.

The Medici guarded against bandits, pirates, wars, greedy lords, and even the church, by using tools of protection that involved stealth and currying favor within the official power structure.[1] In the United States, as banks became closely tied to the government through regulation and policy,[2] bank security concerns shifted from the authorities to private robbers, embezzlers and swindlers who could abscond with bank resources

1. David Abulafia, *The Impact of Italian Banking in the Late Middle Ages and the Renaissance, 1300-1500, in* BANKING, TRADE AND INDUSTRY; EUROPE AMERICA AND ASIA FROM THE THIRTEENTH TO THE TWENTIETH CENTURIES 17, 17-34 (Alice Teichova, et al. eds., 1997).

2. Larry Schweikart, *Banking in North America, 1700-1900, in* BANKING, TRADE AND INDUSTRY; EUROPE, AMERICA AND ASIA FROM THE THIRTEENTH TO THE TWENTIETH CENTURIES , 297, 297-312 (Alice Teichoun, et al. eds., 1997). *See also,* EDWIN HEATHCOTE, BANK BUILDERS 8-23 (2000).

without the possibility of recourse. Now that financial service companies are built on electronic foundations, and now that each company's systems are increasingly interconnected, keeping treasure secure has become a complicated and specialized task.

At the dawn of the third Gregorian millenium, financial service companies face imposing risks ranging from market volatility to balance sheet management, while they respond to the needs of shareholders, customers, communities, employees, markets and government regulators. This paper will address only one set of risks confronting the modern financial services industry: the security risks associated with financial services companies keeping vital financial, business and account information on electronic computing systems connected with public networks. Electronic interconnectivity creates a "shared risk environment" where each participant assumes some responsibility for the security of the entire network. When a business chooses to connect to the public network or to any computer network that contains elements beyond the business' immediate control, the business assumes risks created, condoned, perpetuated or transmitted by other network participants.

Several unique features characterize the current shared risk banking infrastructure. First, information is a financial company's most valuable resource. Money is no longer measured by gold bars, but by notations in a ledger. The data gleaned from customer transactions is an asset to be hoarded or sold. Not only a bank's business secrets, but also its inventory and stock in trade are all stored as information. Second, all vital information is stored and used in electronic formats. Electronic data and records can be counterfeited, copied, broadcast, and analyzed easily, anonymously, and in very large numbers for an intruder with the right tools. Third, computers are connected with outside networks, facilitating access by intruders. Fourth, banks have relinquished most controls on customer access. Financial services customers demand immediate and remote transactional capability from their accounts at all hours of the day. Fifth, financial sophistication has radically amplified business complexity. Banks no longer just take deposits and lend cash; now banks sell mutual funds, securities and insurance, underwrite third party risk,

securitize every financial asset, and play in junk bonds, derivatives and real estate investment trusts. Sixth, the work landscape inhabited by modern financial companies is drastically more complicated than in previous decades. Current companies employ a mixture of traditional employees, leased employees, contractors, temporary workers, consultants and outsourcing specialists, each with varying levels of access to critical financial information. Seventh, the American banking system is more active than ever before in global finance, subjecting it to security risks from multiple jurisdictions with varying laws.

Clearly, while information security is vital in such a shared risk environment, it can only effectively alleviate limited categories of risk. Global currency or investment risk, for example, can be only modestly affected by tighter security procedures. If your bank invested heavily in the Thai baht, or invested in companies relying on a strong Thai currency, then the 1998 Asian financial crisis would have rocked your bank's financial stability regardless of its security measures. Therefore, because the focus of this article is *security strategies* in a shared risk banking environment, the authors will limit commentary to those risks arising from the seven factors described above only where those risks can be significantly reduced through well-considered information security policies, tools and procedures.

This paper first explores the current state of banking in a shared risk environment. After reviewing the context of early bank security models and the general risks of interconnectivity, the paper addresses which specific features of banking create unique connectivity risks and describes the current regulatory response to these threats. Finally, the authors discuss and recommend strategies for meeting the modern bank's security needs and regulatory requirements.

Financial service companies are spending billions of dollars each year to address the security risks of today's interconnected banking infrastructure. Financial service regulators are devoting significant attention to the pitfalls of shared risk, holding bank boards responsible for knowing the banks' information security needs and for adequately addressing those needs. Shared risk banking, whether telephone banking for consumers, online

treasury management for corporations, or outsourcing key check processing functions, demands new models of security to keep integrity and trust in the American banking system. Because these issues touch every aspect of a bank's business, from contracting to regulatory compliance to customer satisfaction, bank counsel must be sufficiently conversant with them to be able to lead their clients through the labyrinth.

II. BANKING IN A SHARED RISK ENVIRONMENT

A. Traditional Bank Security

The bank robber is a prominent figure of American mythology. In the "wild west" of the late nineteenth century and the depression of the 1930's, real life criminals became famous and even popular for robbing banks.[3] Celebrated in movie and song, these robbers exploited the primary weakness of banking security: its people. "Slick Willie" Sutton claimed he robbed banks "because that's where the money is," and he used guile, stealth, and of course a gun, to complete his crimes.[4] The Dillinger gang robbed several banks throughout the Midwest using brutal force to overpower bank management and security. A Boston gang's legendary robbery of cash and securities from the Brinks company highlighted the dangers of outsourcing security to third party companies. The more recent multi-million dollar theft at armored car company, Loomis Fargo's facility in Charlotte, North Carolina epitomized the common but least romanticized type of security

3. During these eras, many Americans perceived that banks exacerbated economic problems through tight credit policies and that banks acted as instruments of personal destruction for the banks' foreclosures on family farms and businesses.

4. Always polite and well-dressed, Sutton preferred to sneak into a bank while it was closed or attempt his robbery in disguises such as a mailman or postal telegraph messenger. One victim reported that witnessing one of Sutton's robberies was like being at the movies, except that the usher had a gun. *See* Federal Bureau of Investigation, *Famous Cases, at* http://www.fbi.gov/yourfbi/history/famcases/sutton/sutton.htm (last visited Feb. 13, 2001).

breach – the inside job conducted by company employees.[5]

These famous robberies demonstrate security problems faced by traditional banks prior to the electronic age. During that time, a bank's valuable assets consisted of physical objects, such as cash and securities kept in a safe or a customer's jewelry held in safe deposit boxes. While embezzlement could diminish bank assets through creative accounting, most banks' security focused on protecting the object of value locked behind iron doors. Bank executives clearly understood the nature of their obligations in the traditional business environment where concrete physical security guarded physical objects. In short, thicker walls, more guns, honest tellers and simple procedures were all that was needed to protect any bank's trove.

To provide context for a later discussion of security in a shared risk environment, the following paragraphs review traditional security priorities for non-electronic banks. These banks secure physical assets by relying on perimeter defenses and watchful people.

1. Perimeter Defense

Securing a perimeter is the first element of physical protection. Banks build safes with intricate locks and thick walls. They wrap these safes in buildings where access is restricted with double doors and steel cages. This system is the modern day equivalent of a medieval keep surrounded by castle, moat, battlement and more walls, with the object of keeping intruders at bay and isolating ingress and egress for better monitoring. On a much larger scale, the Great Wall of China exemplifies the same principles: your valuables are safe if the bad guys cannot reach them.

Perimeter security not only limits access to valuable property, but also serves a deterrent function. Any wrongdoers wishing to gain access to the protected property are forced to calculate the amount of time and resources needed to breach the

[5] *See* Jeff Diamant, *Easy Money, Hard Time*, CHARLOTTE.COM (CHARLOTTE OBSERVER), http://www.charlotte.com/observer/special/heist/ pub/0905heist.htm (Sep. 4, 1999).

walls and the likelihood of discovery and punishment. In other words, effective perimeter security is equally valuable as a deterrent to attempted theft as it is to thwarting actual attacks. The higher the walls and the deeper the moat, the longer the siege and the more men required to complete the task. Perimeter security is always necessary, but seldom is it sufficient to deter all attempts and thwart access.[6] Protecting a treasure requires more than just thick walls.[7]

2. The Human Element

The most important security problem with valuable physical property is that the property must be accessed for its value to be realized; its value diminishes if it cannot be counted, appraised, admired or spent. Therefore, no matter how thick a safe's walls or how deeply it is buried in the ground, its protector must have some method for the property owners to access their valuables. As exemplified by the famous robbery cases listed above, wrongdoers tend to evade security and reach valuable property the same way its owners would reach the property.[8] The people guarding the property open doors to the robberies.[9] While

---

6. When the prize is great, no wall may be high enough to stop a determined foe. *See* Flavius Josphephus, *The Horrors of the Siege*, THE BOOK OF WAR: 25 CENTURIES OF GREAT WAR WRITING (John Keegan ed., 1999), at 143 (giving a first-hand account of the Roman Siege of Jerusalem in 69 AD). *See also* Andrew Wheatcroft, *The Fall of Constantinople*, THE BOOK OF WAR: 25 CENTURIES OF GREAT WAR WRITING, at 143-167 (covering the attack of the Golden Horn and the Walls of Theodsius in 1453).

7. According to Machiavelli:

> If the walls are built very high, they will be too much exposed to artillery; if they are built very low they may be easily scaled; if you dig a ditch on the outside of the walls to make an escalade more difficult and the enemy should fill it up (which may be done by a numerous army), he will immediately become master of them.

NICCOLÓ MACHIAVELLI, THE ART OF WAR 183 (Neal Wood trans., Da Capo Press) (1965).

8. Willie Sutton would walk into a bank before it opened, dressed as a Western Union messenger, and take the bank guard's gun as he signed for a telegram. After the guard admitted the bank manager, the manager was coerced into opening the safe. *See* QUENTIN REYNOLDS, I, WILLIE SUTTON: THE PERSONAL STORY OF THE MOST DARING BANK ROBBER AND JAIL BREAKER OF OUR TIME (1953), at 110-113.

9. In some cases like the Loomis Fargo heist, the people guarding the property

the movies may show dramatic bank robberies that involve cracking the combination of a safe, blowing a hole in the wall or simply hauling the safe away to be broken at a distant location, real life bank robbers who take physical cash or other objects of value, tend to coerce or pay bank employees to gain standard access to the vaults.

The vulnerabilities associated with the protection of physical property arise from the character of bank employees as well as security procedures implemented by management. Individual bank employees can thwart security in many ways and for many reasons.[10] On one end of the culpability scale, a bank employee may plan and execute a robbery of her employer. On the other end of this scale, the employee may be coerced into assisting the criminal or may unwittingly give away security secrets through innocent but misguided actions or conversation. Even assuming honest and careful people are working at a bank, traditional bank security risks may be affected by company policies. For example, if none of the regular employees at a facility know how to open the vault or certain sections of the vault, then a robber is less likely to gain access. A careful company may implement a policy to limit employees' knowledge of daily security procedures on a need-to-know basis. If fewer people have access to valuable property, then criminals have fewer opportunities for theft. In addition, policies regarding movement of valuable property, storage of the property, accounting, auditing and taking inventory can significantly affect the security of the bank's most valuable physical property.

Prior to the digital revolution, bank security revolved around protecting cash and other physical assets. This protection was accomplished by setting up perimeter security, hiring trusted

---

are themselves the robbers. The Loomis Fargo robbers, who took the second largest cash theft in United States history, included an employee and former employee of the armored car company. Diamant, *supra* note 5. In other cases, the people responsible for guarding the property are coerced or intimidated into allowing access to valuable physical property.

10. See, e.g. Dennis Blank, *When the Hacker is on the Inside: Thousands of Attacks Each Year Come From Current or Former Employees – And Companies Are Only Now Beginning to Step Up Their Defenses*, BUS. WK. ONLINE, *at* http://www.businessweek.com/bwdaily/dnflash/dec2000/nf20001213_253.htm (Dec.13, 2000).

employees and implementing protective policies. While these measures stopped some robberies and deterred many others, the Willie Suttons, John Dillingers, Brinks' robbers, and Loomis Fargo's hijackers represent thousands of others who overcame the security measures, at least for a time.

B. New Risks from Interconnectivity

While the financial world has changed dramatically since Willie Sutton's time, banks are still "where the money is." The threats to banks have increased and the combination of technology, globalization, deregulation and new business methods have made information security infinitely more complex.[11] This section addresses the current state of interconnectivity, the shared risk security model as it relates to banking and relevant business-specific and regulatory security issues currently facing banks.

1. A Glimpse of the New Environment

During the past two decades, banking has drastically changed. Most significant to the discussion of information security, the assets of banks have changed and the access to banks has changed. Much of this shift was driven or permitted by new technology that has allowed money to become information and information to become money. Walter Wriston, former President of Citicorp, is credited with the famous statement "Information about money has become almost as important as money itself."[12] Money has become primarily digital. The net worth of most

11. Certainly banks and other financial service companies must remain concerned with physical security. People still use guns and physical threats to take money from banks. In addition, physical security is a vital element of sensible information security. For example, a criminal could create havoc and learn valuable information by walking into a financial company and stealing an entire network server or key manager's personal computer (although system security such as screen locks and encryption may thwart the attempt). However, this paper concentrates on the electronic threats to information and the strategies designed to meet these new threats.

12. Nikki Goth Itoi, *Wriston Watch: Walter Wriston on the Role of Technology and Finance*, RED HERRING, Oct. 1998, at 63. This quotation is also inscribed in the lobby of New York Science, Industry and Business Library.

companies and individuals in today's society is measured in electronic ledger notations, rather than physical goods. A person's bank accounts, security holdings, and credit line are kept electronically by financial institutions. Therefore, money is now information.

But information is also money. "Banking has never truly been about finance... It has been about access to information about finance."[13] Financial services companies are building massive databases with information about customers, their accounts, their preferences, and their financial habits. As more consumers build multiple relationships with their banks,[14] these databases become more powerful and more valuable.[15] Walter Wriston made the following observation about the data mining capability of banks:

> The ability to have a huge database that a bank can mine in real time means that when a bank calls a customer, it knows that you've got a checking account at the bank, that there are two CDs in safe-deposit box, that you use their brokerage system, that your income is x dollars, and that you live down by the Embarcadero.[16]

---

13. David J. Wallace, *Business to Business; The Internet Gives Corporate Banking a Do-It-Yourself Look*, N.Y. TIMES, Dec. 13, 2000, at 4. Mr. Wallace continued "The Internet allows information flow instantly between the parties in a transaction. Early systems had built-in delays because of mail, fax or phone delivery, and multiple levels of management needed to approve payment. Using open Internet standards, participants can revise an invoice anywhere a Web connection exists." *Id.*

14. In June [1998], Forrester Research conducted a survey of 120,000 consumers in North America. The survey revealed that 64% of consumers would choose a bank to consolidate their financial services, while less than 1% would switch to a technology company that offered one-stop financial services shopping under its own name. Nikki Goth Itoi, *Breaking the Bank: Technology is Forcing Banks to Become Nimble Financial Service Aggregators that Cater to Customers Through a Variety of Electronic Channels – Because If They Don't, Yahoo and Intuit Will*, RED HERRING, Oct. 1998, at 64.

15. Jane Kaufman Winn & James R. Wrathall, *Who Owns the Customer? The Emerging Law of Commercial Transactions in Electronic Customer Data*, 56 BUS. L. 213, 213-87 (2000). The article gives a detailed discussion of consumer databases (especially pp. 230-38) as well as database case studies and legal analysis of privacy issues. *Id.*

16. *See* Itoi, *Wriston Watch: Walter Wriston on the Role of Technology and Finance, supra* note 12, at 63.

Banks currently use this customer data to improve customer service and to more directly target marketing of financial services to customers likely to be interested in purchasing those services. This information about money is extraordinarily valuable to banks.[17]

Compounding the changes wrought by the information revolution is the interconnectivity revolution. Banks are no longer simply isolated fortresses with thick walls and armed guards. In fact, many current banks have no physical presence whatsoever.[18] The internal bank networks that arose through the late 1980's and early 1990's became connected with each other. These networks were also connected with public networks in the mid to late 1990's.[19] As a result, not only have significant bank assets been

17. For example,

> The combination of larger, more robust customer databases and sophisticated data warehousing and mining technology can offer substantial competitive advantages to electronic commerce businesses. Companies can develop the ability to better identify likely customers and to recognize and anticipate individual preferences, resulting in increased sales and higher margins. In addition, once it is assembled, a customer database may be shared with other companies, offering an additional revenue stream at a low incremental cost.

Winn & Wrathall, *supra* note 15, at 235-36.

18. *See* Vanessa Richardson, *Breaking the Virtual Bank,* REDHERRING.COM (Feb. 22, 2000), *at* http://www.redherring.com/vc/2000/0222/vc-onlinebanks022200.html (last visited Mar. 3, 2001). Richardson states that at the time of the writing there were "currently more than 30 Internet banks in operation." *Id.* She cites Dataquest as predicting that "one-third of the 60 to 100 new online banks will fail within the next three years." *Id. See also,* THOMAS P. VARTANIAN, REMOTE BANKING AND FINANCIAL SERVICES (2000). Vartanian provides an in-depth discussion of all aspects of remote banking. He describes a company known as TeleBank based in Arlington, Virginia, which has no physical branches and its customers bank exclusively by phone and by mail. *Id.* TeleBank was acquired in January 2000 by ETRADE Group, Inc. and is now known as ETRADE Bank. *Id.*

19. According to *Breaking the Bank,*

> In the early 90s, banks typically spent most of their technology budgets on systems for employee use and for upgrades and maintenance of existing facilities – that is, on internal development. Only about three percent was funneled into external development of new systems.... By 1995, when U.S. industry-wide technology spending measured about 25 billion dollars, the percentage dedicated to external IT projects had risen

moved to a digital format,[20] but anyone with access to public networks can attempt to reach that value. Clearly, in this new world order, banks must have more than perimeter-based security to address the risks of valuable assets.

There is no turning back. Bank customers are demanding the instant 24-hour access and better financial control offered by digital banks connected to public networks. Robert Sterling, an analyst with Juniper Communications, was quoted in the New York Times stating that approximately 10% of American consumers bank online and in 1999, 8.3 million people shopped for mortgages and other loans on the internet, with one of eight starting the loan application process online.[21] At the time of this writing, Bank of America claims over three million online banking customers, and Wells Fargo claims more than two million banking customers.[22]

Bankers with digital assets in a networked world must assess the new banking risks and meet them with new security measures.

2. The Shared Risk Security Model

Computers connect into networks and computer users share the security risks. When a wrongdoer breaks into one computer or server, he may be able to access any other computer on the network. As computers in all industries and sectors tie together, bringing new value to the system, new vulnerabilities

---

> to 20%, or 4.3 billion dollars. Gary Craft, an analyst with BankAmerica Robertson Stephens, believes that the figure will approach 8.6 billion by 2000.

Itoi, *Breaking the Bank*, *supra* note 13, at 62.

20. As much as 600 billion dollars of the market value represented by today's financial service companies may eventually be moved online. *See* Richardson, *supra* note 18.

21. Patrick McGeehan, *Personal Finance; Banks are Slow to Move Online, But So Are Their Customers*, N. Y. TIMES, June 7, 2000, at H6.

22. Press Release, Bank of America, Bank of America Exceeds 3 Million Online Banking Customers, http://www.bankofamerica.com/newsroom/press/press.cfm?PressID=press.2001009.01.htm (Jan. 9, 2001); Press Release, Wells Fargo, Wells Fargo First Major Bank To Launch Nationwide Wireless Banking, at http://www.wellsfargo.com/press/press010207.jhtml;$sessionid$5VCGUFYAAIUY4CQMKVDFARQKBRKTMUMO (Feb. 7, 2001).

follow.[23] In testifying before the United States Congress regarding protection of information infrastructure, Deputy Secretary of Defense John J. Hamre stated that "As . . . Services and Agencies interconnect more of their networks, we are creating a shared risk environment. In a shared risk environment, the security posture of the interconnected systems is only as great as the system with the weakest assurance posture – in effect, the weakest link in the chain."[24] While customers demand interconnectivity and banks profit from the networked computer infrastructure, the shared risk environment ensures that weakness in one node may be exploited throughout the system.[25] In today's seamless worldwide web,

---

23. "As a result of advances in information technology and the necessity of improved efficiency . . . [critical national] infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks." Presidential Decision Directive 63, The Clinton Administration's Policy on Critical Infrastructure Protection, May 22, 1998, *available at* http://www.ciao.gov/CIAO_Document_Library/paper598.pdf (last visited Mar. 3, 2001) [hereinafter Clinton White Paper on Critical Infrastructure Protection].

24. *Briefing on Information Assurance and Critical Infrastructure Protection Before The Subcommittee on Procurement and R&D of the House National Security Committee*, 105th Cong. (1998) (testimony of John J. Hamre, Deputy Secretary of Defense).

25. It has been noted that,

> [I]n addition to its benefits, this widespread interconnectivity poses enormous risks to our computer systems and, more importantly, to the critical operations and infrastructures they support .... Our nation's computer-based critical infrastructures are at increasing risk of severe disruption. Interconnectivity increases the risk that problems affecting one system will also affect other interconnected systems. Massive computer networks provide pathways among systems that, if not properly secured, can be used to gain unauthorized access to data and operations from remote locations. While the threats or sources of these problems can include natural disasters, such as earthquakes, and system-induced problems . . . government officials are increasingly concerned about attacks from individuals and groups with malicious intentions, such as terrorists and nations engaging in information warfare.

UNITED STATES GENERAL ACCOUNTING OFFICE, CRITICAL INFRASTRUCTURE PROTECTION 3 (1999).

"Given the risks and the fact that weakness in any portion of our network is a threat to the operational readiness of all connections, our Information Assurance goal is to ensure the continuous availability of our systems and networks." *Computer Security: Cyber Attacks – War without Borders: Hearings Before the Subcomm. for Gov't Mgmt., Info. and Tech. of the House Gov't Reform Comm.*, 106th Cong. (2000) (testimony of Mario Balakgie, Chief Information Assurance Officer, Defense

electronic threats can rise from across the globe as easily as from next door.[26] Understanding the peril faced by today's networked financial services companies requires examining the types of risk caused by their infrastructure and exploring the current inadequacies of the law.

a. Defining Financial Services Risk

Banks are faced with innumerable risks arising from their interconnected computer networks. Because of this risk, regulators charged with examining and protecting the financial services industry have carefully categorized the types of risk faced by banks. Based on the risks, associated with their business and technology, banks are required to evaluate their own performance and underlying strengths.

Other measures of risk can also help banks understand the threats to earnings, capital and stability. Federal Bureau of Investigation (FBI) Director Louis Freeh testified before the United States Senate Judiciary Committee last year, noting the explosive growth in computer intrusion cases handled by the FBI.[27]

Intelligence Agency, Department of Defense).

26. Janet Reno commented:

> As people can sit in a kitchen in St. Petersburg, Russia and steal from a bank in Chicago, ... as people can extort people halfway around the world, how will we build a partnership with our colleagues around the world to track these people, to bring them to justice and to make again the opportunities of the internet real for the world?

United States Attorney General Janet Reno, Address at the Cybercrime Summit: A Law Enforcement/Information Technology Industry Dialogue on Prevention, Detection, Investigation and Cooperation at the Stanford University Law School (Apr. 5, 2000).

27. *Statement on Cybercrime: Hearings on S.*2092 *Before the Subcomm. for Tech., Terrorism and Gov't Info. of the Senate Judiciary Comm.*, 106th Cong (2000) (testimony of Louis J. Freeh, Director United States Federal Bureau of Investigation), http://www.fbi.gov/pressrm/congress/congress00/cyber032800.htm (last visited Feb. 27, 2001) [hereinafter Freeh Testimony]. Director Freeh reported:

> Our caseload is increasing dramatically. In FY 1998, we opened 547 computer intrusion cases; in FY 1999, that had jumped to 1154. At the same time, because of the opening the National Infrastructure Protection Center (NIAC) in February 1998, and our improving ability to fight cyber crime, we closed more cases.

Freeh told the Committee that ninety percent of the companies in private survey reported security breaches and at least seventy-four percent of the companies reported "security breaches including theft of proprietary information, financial fraud, system penetration by outsiders, data or network sabotage, or denial of service attacks."[28] This survey obviously did not report the large number of computer intrusions that go undetected. Director Freeh then described for the Committee some of the categories of specific electronic threats faced by American business and government in 2000. He included threats from insiders,[29] hackers (or crackers),[30] virus writers,[31] criminal groups,[32] terrorists,[33] foreign

---

> In FY 1998, we closed 399 intrusion cases, and in FY 1999, we closed 912 such cases. However, given the exponential increase in the number of cases opened, cited above, our actual number of pending cases has increased by 39 percent, from 601 at the end of FY 1998, to 834 at the end of FY 1999. In short, even though we have markedly improved our capabilities to fight cyber intrusions, the problem is growing even faster.

Id.

28. *Id. See also, The Internet Integrity and Critical Infrastructure Protection Act: Hearing on* S.2448 *Before the Senate Comm. on the Judiciary,* 106th Cong. (2000).

> Information theft and financial fraud caused the most severe financial losses, put at $68 million and $56 million respectively. The losses from 273 respondents totaled just over $2265 million. Losses traced to denial of service attacks were only $77,000 in 1998, and by 1999 had risen to just $116,250. Further, the new survey reports on numbers taken before the high-profile February attacks against Yahoo, Amazon and eBay.

Id.

29. The Statement on Cybercrime noted:

> The disgruntled insider (a current of former employee of a company) is a principal source of computer crimes for many companies. Insiders' knowledge of the target companies' network often allows them to gain unrestricted access to cause damage to the system or to steal proprietary data. The just-released 2000 survey by the Computer Security Institute and FBI reports that 71% of respondents detected unauthorized access to systems by insiders.

Id.

30. Director Freeh notes that cracking may be attempted "for the thrill of the challenge" or for personal profit. *Id.* He also discusses the rise of politically motivated hacking undertaken to send a message. *Id.*

31. "Virus writers are posing an increasingly serious threat to networks and systems worldwide. Last year saw the proliferation of several destructive computer viruses or 'worms,' including the Melissa Macro Virus, the Explore.Zip worm, and

intelligence services,[34] information warfare,[35] Internet fraud,[36] intellectual property theft,[37] as well as distributed denial of service attacks.[38] The list of threats that the new digitized, interconnected infrastructure has imposed on banking should also include identity theft,[39] spoofing (known as page-jacking)[40] and facilitated money

---

the CIH (Chernobyl) Virus." *Id.*

32. Freeh discusses the international criminal theft conspiracy called the "Phonemasters" who combined physical techniques like dumpster diving and pretext telephone calling (often referred to as "social engineering") with computer system penetration to steal calling card numbers. *Id.* He also uses the example of the gang of thieves led by Vladimir Levin, a Russian computer expert who illegally transferred more than $10 million from Citibank corporate customers. *Id.*

33. Freeh's testimony also states:

> Terrorists groups are increasingly using new information technology and the Internet to formulate plans, raise funds, spread propaganda and to communicate securely... While we have not yet seen these groups employ cyber tools as a weapon to use against critical infrastructures, their reliance on information technology and acquisition of computer expertise are clear warning signs. Moreover, we have seen other terrorist groups...engage in attacks on foreign government web-sites and email servers.

Freeh Testimony, *supra* note 27.

34. Freeh was coy in delineating this threat. "While I cannot go into specifics about more recent [than 1986] developments in an open hearing, it should not surprise anyone to hear that foreign intelligence services increasingly view computer intrusions as a useful tool for acquiring sensitive U.S. government and private sector information." *Id.*

35. "The prospect of 'information warfare' by foreign militaries against our critical infrastructures is perhaps the greatest potential cyber threat to our national security. We know that several foreign nations are developing information warfare doctrine, programs, and capabilities for use against the United States and other nations." *Id.*

36. Freeh uses this category to describe consumer-oriented fraud schemes using the Internet as a communications medium. *Id.*

37. Freeh limits this discussion to pirated digitized products like software, music and movies using the Internet as a distribution medium. *Id.* He does not address a type of intellectual property theft relevant to the financial services industry, the loss of trade secrets and other proprietary information using the Internet as an access tool to enter bank business systems, or as a broadcast tool for a disgruntled employee. *Id.*

38. Freeh notes that:

> [H]ackers plant tools... on a number of unwitting victim systems. Then when the hacker sends the command, the victim systems in turn begin sending messages against a target system. The target system is overwhelmed with the traffic and is unable to function. Users trying to access that system are denied its service.

Id.

39. Identity theft pertains to obtaining and using individual consumer financial

laundering.[41]

As demonstrated above, the risks now facing banks are infinitely more complicated than Willie Sutton at the door with a gun. The new Willie Sutton may be an ocean and half a continent away from the bank when he breaks into the electronic vault. Or the new threat may rise because the bank is an important link in the American critical infrastructure, and thus a political threat, rather than just a money repository.[42] The next section examines risks associated with this complexity by reviewing the features of the new technology that create identifiable risk.

b. Security Risks Rising from Networked Digital Information

The Internet contains several unique features as a business tool that present new security challenges for financial services institutions. The most obvious is two-way connectivity. Unlike

---

information to engage in fraudulent transactions. *See generally* Exec. Order No. 13133, Appendix A, at 3, 64 C.F.R. 43895 (Aug. 5, 1999), *amended by* Internet False Identification Prevention Act of 2000, Pub. L. No. 106-578, 114 Stat. 3075 (2000). *See also,* Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 (a)(7) (Supp. IV 1998).

40. Page-jacking pertains stealing from other websites descriptions, mega-tags or keywords. *See generally* Exec. Order 13133, *supra* note 39, Appendix A, at 4. Page-jackers places this information on their own site to misdirect users to their site. *Id.* The most dangerous trend in page-jacking is not the common misdirection toward pornographic Internet sites, but the fake bank sites that catch the typing mistake of an unsuspecting consumer and then, posing as the legitimate bank's Web site, requests the consumer's personal account information. "As long as a bank's Web site looks professional and has effective navigation, customers perceive it as secure." Olga Kharif, *Sounding the Alarm over Fake Bank Sites,* BUS. WK. ONLINE (Aug. 7, 2000), *at* http://www.businessweek.com/print/bwdaily/dnflash/aug2000/nf2000087_172.htm (quoting Cheskin Research partner Steve Diller) (last visited Feb. 27, 2001). "When typing their passwords at a false bank site, customers could give hackers access to the real bank – and their accounts. Ensuring authenticity of the bank, the customer, and of each transaction is the online banking industry's most pressing concern now . . ." *Id.* (quoting Richard Mack, manager at RSA Security).

41. *See* Christopher D. Hoffman, *Encrypted Digital Cash Transfers: Why Traditional Money Laundering Controls May Fail Without Uniform Cryptography Regulations*, 21 FORDHAM INT'L. L. J., 799 (1998).

42. Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. Clinton White Paper on Critical Infrastructure Protection, *supra* note 23, at 1. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. *Id.*

media such as television, radio or newspapers, the Internet allows interactive tools such as email, chat, order forms and immediate response functions. Unlike other one-to-one communication media like telephone or telegraph, the Internet allows one person to publish for a mass audience. Unlike all other media, the Internet permits any person with an electronic connection to have immediate, interactive access to the infrastructure of business and government. Just as retail businesses for centuries have kept their doors open to encourage customers, banks allow connections to the Internet to facilitate communication and file sharing. But the open door may also bring the undesirable bugs, rats and brigands into the bank. This unprecedented electronic access occurs at the point in history when banks are consolidating their most valuable assets – money, securities, intellectual property and customer databases – as information in electronic formats. Banks may be storing these valuables where they may be reached from the Internet. Creative methods of reaching secret information[43] are only matched by the creative ways people find to make mischief with the information.[44]

Another useful but dangerous function of networked electronic information is the digitization itself. Digital information, whether movies, software or personal checks, can be easily duplicated with no degradation in future generations of duplicates. Furthermore, through use of encryption, communication of the digital information can be anonymous, allowing unlimited and untraceable copies of products, programs and promissory notes. Banks are accustomed to managing a certain degree of anonymity; cash is anonymous and other paper instruments of value, like bearer bonds, may be traded anonymously. Several electronic systems are moving toward the goal of anonymous digital cash.[45]

43. *See, e.g.*, Mike Brunker, *Vast Online Credit Card Theft Revealed: Hacker Hid Data on 485,000 Cards on U.S. Agency's Web Site*, MSNBC.com, http://www.msnbc.com/news/382561.asp (Mar. 17, 2001).

44. *See, e.g.*, Alex Salkever, *Cyber-Extortion: When Data is Held Hostage*, BUS WK. ONLINE (Aug. 22, 2000), *at* http://www.businessweek.com/print/bwdaily/dnflash/aug2000/nf20000822_308.htm (last visited Feb. 27, 2001) (reporting two Russian computer experts tried to charge Bloomberg $200,000 in "consulting" fees to privately reveal how to compromise the Bloomberg computer systems).

45. *See generally* Hoffman, *supra* note 41. Hoffman discusses various technologies and systems supporting a movement toward digital cash. He includes

However, the easy duplication and anonymity of electronic information on the Internet, even electronic cash, create security problems for financial services companies.[46] Anonymous transactions and easily duplicated targets give cover to thieves, terrorists and money launderers.[47] Furthermore, law enforcement officials may be uncomfortable with anonymity in the financial system, and financial service providers may be required to strip some of the anonymity from electronic financial transactions.[48]

For decades, one of a bank's most important security measures has been careful accounting. Trustworthy record keeping thwarted embezzlement and caught sneaky robbers. The digital financial infrastructure has made financial accounting both easier and more difficult. Automated accounting allows the

---

analysis of digital coins, stored value cards and key escrow cryptography, before leaping into an examination of laundering digital money. Hoffman states:

> The most dangerous aspects of electronic money making it conducive to money laundering are its speed and anonymity. Fortified by cryptography, electronic money precludes retracing the countless transfers in the layering and placement stages of the laundering process... Conducted outside the regulated network of financial institution, such transfers may thwart current measures enacted to prevent money laundering unless law enforcement officials can trace the funds without relying on paper trails.

Id. at 845-846.

46. "Anonymous communication is a great tool for evading detection of illegal and immoral activity. Conspiracy, electronic hate-mail and hate-speech in general, electronic stalking, libel, general nastiness, disclosure of trade secrets and other valuable intellectual property, all become lower-risk activities if conducted via anonymous communications." A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J. L. & COM., 395, 402 (1996).

47. Freeh stated that:

> [O]ne of the largest challenges to FBI computer investigative capabilities lies in the increasingly widespread use of strong encryption... [which] has placed a tremendous burden on the FBI's electronic surveillance technologies. Today the most basic communications employ layers of protocols, formatting, compression and proprietary coding that were non-existent only a few years ago.

Freeh testimony, *supra* note 27.

48. Froomkin, *supra* note 48, at 399. Froomkin suggests "that governments may be able to control anonymous commerce by concentrating on financial service providers. Financial service providers are already highly regulated, and present a relatively easy target for governments seeking to prevent fully anonymous fund transfers." *Id.* at 400-01.

computer to perform rote functions and removes human error from many administrative functions. However, when a company automates its books, its accountants step further away from the actual counting as the institution places faith in the technology. Clever criminals who understand the technology may steal a bank's money with a simple transfer order through a glitch in the accounting software, removing all need for the physical action required for a bank robbery. By the time accountants discover a software problem (if they ever do), the criminal may have long ago disappeared from the bank's systems and records, while the money may have bounced electronically through ten different countries. Electronic record keeping combined with electronic transfer procedures can lead to bank robbery from a living room miles away.

To take full advantage of cost savings and accessibility improvements offered by electronic commerce, financial services companies must be able to contract electronically. In other words, a business will lose transactions and pay more money to process transactions if sales initiated on the Internet must be completed on paper.[49] But electronic contracting creates a new level of security risk for financial institutions. First, the fundamental legal framework must provide certainty that electronic contracts will be treated the same as paper contracts under the eyes of the law and as an evidentiary matter in court.[50] The United States federal

49. Geanne Rosenberg, *Legal Uncertainty Clouds Status of Contracts on Internet*, N.Y. TIMES, July 7, 1997 at D1.

50. Andrew J. Pincus, General Counselof the United States Department of Commerce, described the legal framework surrounding electrionic signatures:

> The basic legal framework needed to enable electronic transactions in a commercial context consists of two essential elements. First is the elimination of statutory rules requiring paper contracts. There is a broad consensus that – with the exception of a few specialized agreements (wills and property deeds, for example) – parties' electronic agreements should have the same legal status as paper agreements.
>
> The second element involves when and how an electronic commercial contract becomes legally binding on, and therefore enforceable in court against, a person or entity that is a party to the contract. In the off-line world, the key question is whether a party has manifested its intent to be bound by the contract, which generally occurs through a written record, and often, affixing a

government and several states attempted to provide legal certainty in electronic contracting by passing digital signature laws.[51] A secured transaction of information must have the following five characteristics: (1) identification of the parties; (2) privacy; (3) authentication; (4) integrity; and (5) non-repudiation.[52] While clear and comprehensive digital signature laws may assist in assuring non-repudiation of electronic contracts, these laws do not affect the other requirements for a secured transaction. Electronic contracting will continue to raise security and enforceability problems for financial service institutions until the laws are completely settled and the market agrees on a safe, easy and inexpensive cryptography regime to assure identification and privacy of the parties, authentication of the transaction and assurance of its integrity.[53]

Finally, the combination of electronic accounting systems, electronic storage of value, electronic documents, and immediate, constant electronic connections with customers and vendors allow banks to manage more assets and more transactions in more financial arenas than ever before. This provides more opportunities for shareholder profit. However, the complexity

---

> written signature to that written record. A signature, however, often is not a legal requirement (for example, a binding contract may be formed through an exchange of telegrams).

Electronic Signatures in Global and National Commerce Act: Hearings on H.R. 1714, Before the Subcomm. on Courts and Intellectual Property on the House Judiciary Comm., 106th Cong. (1999) (testimony of Andrew J. Pincus, General Counsel, United States Department of Commerce).

51. *See* Electronic Signatures in Global and National Commerce Act, Pub. L. No. 106-299, 114 Stat. 464, 465-473 (2000). *See also,* Ariz. Rev. Stat. §§44-7001 - 44-7051 (2000); Cal. Civil Code §§1633.1 - 1633.17 (West 2000); Del. Code ANN. tit. 6, §§12A-101 - 12A-117 (2000); Fla. Stat. ANN. §668.50 (West 2000); Haw. Rev. Stat. §489E (2000); Idaho Code §28-50 (Michie 2000); Ind. Code §26-2-8; Iowa Code §554D (2001); Kan. Stat. ANN. §§16-1601 - 16-1620 (2000); Me. Rev. Stat. ANN. tit. 10, §§9401 - 9419 (West 2000); Mich. Comp. Laws §§450.831 - 450.849 (2000); Minn. Stat. §325L (2000); Neb. Rev. Stat. §86-2101 - 86-2116 (2000); N.C. Gen. Stat. §66-308 (2000); Ohio Rev. Code ANN. §§1306.01 - 1306.15 (West 2000); Okla. Stat. tit. 12A, §§15-101 - 15-120 (2000); Pa. Stat. ANN. tit. 73, §§ 2260.101-2260.5101 (West 2000); R.I. Gen. Laws §42-127.1 (2000); S.D. Codifided Laws §§53-12-1 - 53-12-50 (2000); Utah Code Ann. §§46-4-101 - 46-4-501 (2000); Va. Code Ann. §§59.1-479 - 59.1-498 (Michie 2000).

52. *See generally* A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49 (1996).

53. *See* Symposium, Financial Services: Security, Privacy and Encryption, 3 B. U. J. SCI. & TECH. L. 4 (1997).

that accompanies this flexibility leads to greater security risks. More complexity means more opportunity for human error, for unobserved machine error, or for financial losses to escape the standard system of controls. More complexity means less people with a broad encompassing knowledge of the entire system and more risk that the secure parts of a bank's infrastructure will not fit together properly. Greater complexity means more misplaced credits and requires a longer time to investigate losses. For example, financial regulators have noted that outsourcing key technical functions is a troublesome business complexity.[54] Outsourcing increases the complexity of managing technology tasks while reducing the control a financial institution maintains over the process.[55] In short, greater complexity can provide a myriad of opportunities for successful and anonymous theft or damage.

c. Current Legal Gaps

The law lags, rather than leads, society. So while networked digital information rapidly pervades our homes and businesses, the law moves slowly in its wake, addressing issues as they reach courts or create public outrage. Gaps between the realities of the shared-risk infrastructure and the current state of law magnify security risks faced by banks. The United States

54. *FFIEC Guidance on Managing Risks Associated With Outsourcing Technology Services*, [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 60-707 (FDIC FIN. INST. LETTER 81-2000, Nov. 29, 2000), *available at* http://www.fdic.gov/news/news/financial/2000/fil0081.html (last visited Mar. 3, 2001).

55. Risks of outsourcing information and transaction processing and settlement activities include:

> [t]hreats to security, availability and integrity of systems and resources, confidentiality of information, and regulatory compliance.... Management should consider additional risk management controls when services involve the use of the Internet. The broad geographic reach, ease of access, and anonymity of the Internet require close attention to maintaining secure systems, intrusion detection and reporting systems, and customer authentication, verification and authorization.

Id. at 2. The FDIC letter notes that bank managers should pay special attention to 1) due diligence in selecting a service provider, 2) contract requirements of that service provider, and 3) continuing oversight of that service provider. *Id.*

Congress has recently passed legislation regarding electronic contracting and consumer privacy in financial information.[56] However, recent Congressional bills relating to the Internet have tended to focus on social and consumer issues,[57] although this federal Internet legislative agenda covers law enforcement issues important to the financial services industry.[58] Despite progress, many areas of American business law remain unclear or unsettled, including multi-state use of electronic signatures,[59] use of encryption,[60] and evidentiary issues.[61] Furthermore, many

56. *See supra* note 51 (electronic signatures) and *infra* note 65 (consumer privacy).

57. The 106th Congress introduced several bills designed to protect children online. *See* Cybermolesters Enforcement Act of 2000, H.R. 4076.IH, S. 2280.IS, 106th Congress (2000); Children's Internet Protection Act, H.R. 543.IH, S. 97.IS, 106th Congress (2000); Student Privacy Protection Act, H.R. 2915.IH, S. 1908.IS, 106th Congress (2000); Children's Protection Act 2000, S. 2127.IS, 106th Congress (2000); Neighborhood Children's Internet Protection Act, S. 1545.IS, 106th Congress (2000). *See also* S. RES. 294.IS, 106th Congress (2000) (designating the month of October 2000 as Children's Internet Safety Month).

58. *See, e.g.,* Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 (Supp. IV 1998) (criminalizing identity theft); Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1994) (penalizing the misuse of information gathered electronically without permission); Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-22, 2701-11 (1994). Although some commentators have argued that even these and related criminal laws protecting digital information should be updated. *See* Freeh Testimony, *supra* note 27, at 10-11 (the FBI supports strengthening "the general deterrence aspects of the Computer Fraud and Abuse Act, and to provide some needed procedural enhancements to help us confront the expanding criminal threat..."). While Congress has addressed Online Securities Fraud, general laws prohibiting fraud can apply to conduct over the Internet as well as traditional situations: *See* 15 U.S.C. § 45(a-n) (1994) (unfair methods of competition); 15 U.S.C. § 52 (a)-(b) (1994) (governing dissemination of false advertisements); 15 U.S.C. § 1644 (a)-(f) (1994) (addressing fraudulent use of credit cards; penalties); 18 U.S.C. § 1341 (1994) (frauds swindles); 18 U.S.C. § 1342 (1994) (addressing ficticious names or addresses); 18 U.S.C. §1344 (1994) (governing bank fraud).

59. State laws may contain different requirements and safe harbors than the federal Electronic Signatures Act and many business owners are unclear which of these state laws are preempted by this federal Act.

60. The Clinton administration has changed its position on export of encryption several times, leaving businesses uncertain on the appropriate use of this protection technology. The inconsistencies in public policy are a result of the tension between the need for secure methods to conduct legitimate business online and law-enforcement's desire to deny electronic privacy to criminals and terrorists. S*ee, e.g.,* F. Lynn McNulty, *Encryption's Importance to Economic and Infrastructure Security,* 9 DUKE J. COMP. & INT'L L., 430, 430-48 (1999) (discussing United States and international approaches to cryptography policy).

61. Digital information can be altered in such a way that destroys its evidentiary value, and courts have not conclusively ruled how such evidence will be treated.

computer hackers invading business and government systems are juveniles, and current U.S. law may hinder prosecution of juvenile attackers.[62] As a final point, the digital economy is global in scale and reach, and international legal inconsistencies provide additional security risks to financial services companies. Many nations have not passed laws that prohibit crimes against electronic information systems.[63] Furthermore, businesses in the United States may find barriers to investigation and prosecution of computer crimes committed from personal computers or servers located in other countries.[64] Financial institutions face security

---

62. Freeh Testimony, *supra* note 27, at 10 (explaining even though 18 U.S.C. § 1030 (1994) does not currently allow for the prosecution of juveniles who commit computer violations, S. 2092 would permit the Attorney General to prosecute juveniles for certain felony violations of 18 U.S.C. § 1030 (1994)).

63. According to the McConnell International study on cybercrimes:

> [T]he laws of most countries do not clearly prohibit cyber crimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their 'virtual' counterparts. Web pages such as the e-commerce sites recently hit by widespread, distributed denial of service attacks may not be covered by outdated laws as protected forms of property. New kinds of crimes can fall between the cracks, as the Philippines learned when it attempted to prosecute the perpetrator of the May 2000 Love Bug virus, which caused billions of dollars of damage worldwide.

MCCONNELL INTERNATIONAL, CYBER CRIME... AND PUNISHMENT? ARCHAIC LAWS THREATEN GLOBAL INFORMATION, at 2 (Dec. 2000), *available at* http://www.mcconnellinternational.com/services/CyberCrime.pdf (last visited Mar. 3, 2001). The McConnell International study surveyed fifty-two countries, ten of which had laws allowing the prosecution of perpetrators of data crimes, network crimes, access crimes and related crimes like computer-related fraud (McConnell refers to these countries as having "substantially or fully updated laws"). *Id.* at 4. Nine of the surveyed countries had "partially updated" laws, while McConnell found no "updated laws" for the remaining thirty-three surveyed countries. *Id.*

64. A report from the Department of Justice explains that:

> As a result [of worldwide computer linkages], a criminal no longer needs to be at the actual scene of the crime (or within 1,000 miles, for that matter) to prey on his or her victims... Long-distance detection, however, may take the investigation and prosecution of these crimes out of the exclusive purview of any single jurisdiction, thereby creating yet other challenges and obstacles to crime-solving.

U.S. DEP'T OF JUSTICE, PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET, THE ELECTRONIC FRONTEER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET (Mar. 2000), http://www.usdoj.gov/criminal/cybercrime/unlawful.pdf (last visited Mar. 3, 2001), *at*

hazards caused by uncertainty and inconsistency in the law regarding crimes against information systems and networks. Aside from these new general risks arising from the shared-risk infrastructure, banking institutions must consider their specific new products and business methods to determine how each one affects their security posture. Financial institutions and their regulators are currently wrestling with proposed solutions to risks emerging from networked digital information.

C. *Current Supervisory Issues in a Shared Risk Banking Environment*

1. The Shared Risk Implications of Bank-Customer Connectivity

As discussed above, it is accepted wisdom that there have been profound changes in the business of banking, and in the financial services industry generally, in recent years. The range and sophistication of the products and services offered by banks has expanded considerably, affiliations of banks with other types of financial service providers are now permitted, and banking services are available to customers on a 24 hour/7 day-a-week basis, from any number of delivery channels. Willie Sutton may be hard pressed even to recognize a bank at the onset of the 21st century.

These profound changes, however, have been largely changes of structure and process. The core of the banking business, meanwhile, remains what it always has been: the connection between banker and customer. Banking continues to be a relationship business, entirely dependent upon the communication of information between a bank and its customer. That information can take many forms: the identification of the

20-21. *See also* Mike Brunker, *E-business vs. the Perfect Cybercrime: U.S. Authorities Can't Touch Credit Card Fraud From Overseas,* Mar. 3, 2001, at http://www.msnbc.com/new/376973.asp (last visited Feb. 21, 2001) (reporting that "[a]n investigation by MSNBC has learned that while criminals based overseas now account for up to a third of all online fraud directed at U.S. e-businesses, there is no evidence that a single one of these crooks has been prosecuted").

customer; the bank's condition and competence; the articulation of the customer's needs and the bank's ability to satisfy those needs; the information necessary for the bank to assess the customer's creditworthiness; the agreed-upon terms of a transaction between bank and customer; or the transmittal of monetary value in the form of cash or debit and credit entries. Thus, at its essence, a bank deals in the transmission of information between itself and its customers.

It is the ability of the bank and its customer to connect through various means of communication that makes this transmission of information possible and enables the business of banking to be conducted. This concept of interconnectivity is also at the center of the current supervisory concerns over risk and the appropriate allocation of risk within the banking industry. These concerns have centered on the proliferation of available means of communication or "delivery channels" between the bank and its customers and the vulnerability of those channels to error, compromise or failure.

A fascinating feature of the development of new delivery channels for bank customers is that as more means of interconnectivity between the bank and its customers have been made available, more and more control over those means has been ceded by the bank to the customer. For example, several decades ago, banking was conducted almost exclusively in person at a bank's offices during the bank's (usually rather abbreviated) banking hours. The bank controlled the means of connectivity almost exclusively; the delivery channel was the bank's brick-and-mortar facilities, where a customer's account information was kept in tangible form (remember passbook accounts?) and the channel was open only when the banker was in the office. Contrast that with contemporary banking, in which the delivery channels are many and varied, are remote and virtual (telephone access and web-based communications are examples), and are available upon the customer's initiation and in many cases whenever the customer wants them, around-the-clock. Thus, the rules of connectivity have come to be determined more by the customer than by the bank. The product of this shift of control over the means of connectivity is that banking has become more of a shared-risk

environment. Because banks have had to permit the bank-customer interface to migrate further from the bank's traditional security perimeter, it has become increasingly difficult for banks to recognize, assess and protect against risks of mistake, fraud and intrusion.

2. Risks to Banks of Increased Interconnectivity

Regardless of the delivery channel used, an increase in the ease and frequency with which customers can access information resident in a bank's database necessarily involves a trade-off of security and control of that information.[65] As banks (along with businesses of all types) implement high-technology systems that give customers and potential customers ease of access, several major types of unauthorized activity render these systems particularly vulnerable. They are (1) *hacking*, in which an intruder breaks into a system either for mischief or just to prove it can be done; (2) *identity theft*, through which an intruder captures a customer's unique identifying information (account numbers, social security number, address, phone number, etc.) for use in fraudulent transactions, either with the bank or otherwise; (3) *spoofing*, by which an intruder electronically poses as the bank's server in order to capture identifiers, passwords and other information from an authorized user attempting to access the

65. There are several types of risk that this article will not address. One topic not discussed herein, but that has received abundant attention from industry observers and the regulatory agencies themselves, is that of customer information privacy and security in the context of electronic banking. The issues raised by customer expectations of privacy and security in electronic banking transactions are the application of the privacy provisions of Title V of the Gramm-Leach-Bliley Act of 1999 (Pub. L. No. 106-102, 113 Stat. 1338 (1999)), and their implementing regulations to electronic banking, consumer notice and disclosure requirements in a technology setting, the application of recently-adopted agency guidelines on the protection of customer information and a host of other issues are of undeniable importance to banking organizations which impose their own set of risks. Another topic not specifically addressed herein is the disclosure of corporate information on websites and the possible ramifications under the securities laws for posting inaccurate, incomplete or misleading information. A third topic is the potential liability for fraud or for consumer protection or securities law violations that could flow from including a link to another website that posts inaccurate, incomplete or misleading information. The authors believe that, although important, each of these topics is self-contained and better left for separate and more fulsome treatments than possible in the article.

system; (4) *sniffing*, in which a software program is inserted into a system to search for and capture passwords as they pass through the system; and (5) *distributed denial-of-service* attacks, in which a system is overwhelmed with a large number of bogus communication requests, usually generated by an automatic or repeated-dialing software program, with the intent of blocking or disrupting legitimate traffic.[66]

The various modes of connectivity also carry different degrees of convenience/risk trade-offs. Telephone banking, for example, is reasonably safe from intrusion, because it uses a fairly secure technology channel - standard telephone lines. However, the range of services available through telephone banking is quite limited, and telephone communications are still vulnerable to identity theft and spoofing. On-line banking through personal computers, by contrast, makes possible the delivery of a much broader range of services and much greater convenience, because this channel has a greater capacity for information interchange and greater functionality. However, because electronic commerce generally still has something of a Wild West image, on-line banking raises questions in the minds of some customers regarding security and reliability, and the technology is more vulnerable than telephone banking to hacking, denial-of-service attacks and sniffing. Some observers also are concerned that on-line banking can facilitate money laundering activity.

Advanced information gathering, storage and processing technology—what is commonly known as "aggregation services," "data warehousing" and "data mining"—is an outgrowth of technologically sophisticated delivery channels, and presents its own set of risks. Aggregation services and advanced data management techniques can improve the ease and speed of customer transaction processing, and make possible the tailoring of products and services on demand. However, the accumulation in one place of so much detailed information on individual customers, and with communications technology presenting so

66. *See generally* BASEL COMM. ON BANKING SUPERVISION, RISK MGMT. FOR ELEC. BANKING AND ELEC. MONEY ACTIVITIES ("*Risk Management*"), http://www.bis.org/publ/bcbs35.pdf (last updated Mar. 1998). *See also,* discussion *infra* note 80.

many potential entry points to that information that may be vulnerable to intruders, the risks of compromise are considerable. In addition, a bank that uses such advanced information technology is exposed to substantial risk should customers not be adequately informed of the bank's information use and protection policies or should the information be misused or compromised.

Serving as a certificate authority is another activity that presents its own unique risks. Many banks are considering, and a not insignificant number have undertaken, this activity in which the bank serves as a trusted intermediary or third-party escrow agent for information (principally identification) encryption services. This activity is a natural one for banks. A bank that serves as a certificate authority can facilitate electronic commerce transactions for its customers by leveraging its existing relationships and its expertise as a financial intermediary. However, a bank that engages in this type of activity is at the mercy of its security and authorization systems, and by serving as a certification agent takes on an added layer of risk and potential liability.

A bank that embraces delivery channels based on advanced technology also must address a host of administrative risks. One set of risks comes with what might be called "back-end" relationships. These are the issues that arise in relationships with vendors and outsourced service providers. Because electronic banking involves the use of new, evolving technologies that are marked by rapid change, it frequently is beyond the capabilities of the bank, or not a good use of bank resources, to support these technologies in-house. This evolving technology leads to the purchase of off-the-shelf systems from vendors or the use of outsourcing to third parties to support the bank's efforts. The vendors or outsource contractors therefore assume the role of experts upon whom the bank relies for the proper functioning of these systems. The vendors and contractors bear the risk of performing as promised, and the bank bears the risk that they will perform as promised.

Another set of risks arises in the context of mergers and acquisitions. A bank that comes to rely heavily on sophisticated systems and networks to connect with its customers and its

vendors/contractors faces potentially enormous integration problems following consummation of a merger or acquisition. It is not uncommon for merging organizations to have incompatible systems, and the integration of those systems can be the most difficult task faced by the merger partners. Integration problems carry the risks of customer inconvenience, loss of business and the need to implement expensive fixes for the problems.

Finally, a bank that implements high-technology systems inevitably has to deal with intellectual property issues. The use of advanced technology generates a need for the bank to take appropriate steps both to protect its own intellectual property rights and to avoid infringement of others. With the rapid pace of change in technology development and the proliferation of systems of every kind and description, avoiding the land mines on intellectual property becomes increasingly difficult.

3. The Impact of Risk-Based Supervision

As seen from the foregoing discussion, the nature and multitude of risks that the Internet and other technology-based delivery channels present for banks and other financial service providers is daunting. It therefore is not surprising that the global financial regulatory community has paid particular attention to the issue of information technology risk. This focus also is entirely consistent with the bank regulatory agencies' migration over the past decade from largely transaction-based examinations to a risk-based supervisory approach.

Some decades ago, bank examiners would spend a considerable amount of examination time counting cash in the tellers' drawers. Over time, examiner resources were redirected to higher-level transaction-based examination tasks, such as the review of individual loan files and board minutes. Even that level of micro-examination, however, had become more difficult to justify as institutions became increasingly more sophisticated and complex, incorporating derivatives, securities, a variety of off-balance sheet products and electronic banking into their core businesses. As the Board of Governors of the Federal Reserve System ("Federal Reserve") noted in 1996:

> [A]s evolving financial instruments and markets have enabled banking organizations to rapidly reposition their portfolio risk exposures, it has become clear that periodic assessments of the condition of financial institutions based on transaction testing alone cannot keep pace with the moment-to-moment changes occurring in financial risk profiles. Consequently, in order to ensure that institutions have in place the processes necessary to identify, measure, monitor, and control their risk exposures, examinations and inspections have increasingly placed a greater emphasis on evaluating the appropriateness of such processes and had been evolving away from a very high degree of transaction testing.[67]

As a result, risk-based supervision has assumed an increasingly important role in the supervisory policies and procedures adopted by banking regulators both in the U.S. and abroad. Thus, the bank supervisory agencies have moved toward systemic examination and supervision, with an attendant emphasis on the identification of risk and the implementation of internal control systems to manage that risk. Reliance on the old style of supervision, which essentially was examination by hindsight, has largely fallen from favor. The regulators have concluded that it does not do much good to find problems after they have happened, especially at a time when banks can transmit and deploy vast sums electronically in the twinkling of an eye, or though complex off-balance sheet devices. Risk-based supervision, in the view of the regulators, makes for a forward-looking, proactive supervisory program. In the United States, the Office of the Controller of the Currency ("OCC") officially introduced its program of "Supervision by Risk" its "Community Bank

67. *Interagency Statement on The Effect of Year 2000 on Computer Systems*, Fed. Res. SR Letter 96-16, July 3, 1996, http://www.federalreserve.gov/boarddocs/SRLETTERS/1996/SR9616.htm (last visited Mar. 3, 2001).

Examination Procedures for Noncomplex Banks."[68] There followed in December 1996 the OCC's release of its "Bank Supervision Process" handbook,[69] which described nine risk categories by which the quantity and quality of risk management could be measured.[70] Similarly, the Federal Reserve introduced a rating system for the adequacy of risk management processes and internal controls in November 1995.[71] In November 1996, the Federal Reserve, the Conference of State Bank Supervisors, and the Federal Deposit Insurance Corporation ("FDIC") issued the "State/Federal Supervisory Protocol and Model Agreement,"[72] which contemplates a coordinated risk-focused process of supervision for interstate banks. And in August 1997, the Federal Reserve issued its "Risk-Focused Framework for Supervision of Large Complex Institutions"[73] and "Risk-Focused Framework for Supervision of Community Banks."[74]

4. Guidance from the Basel Committee

Consistent with the move toward risk-based supervision generally, examination and supervision policies relating to information technology and electronic banking activities likewise

68. THE COMPTROLLER'S HANDBOOK, COMMUNITY BANK EXAMINATION PROCEDURES FOR NONCOMPLEX BANKS (Oct. 1995).

69. THE COMPTROLLER'S HANDBOOK, BANK SUPERVISION PROCESS (Apr. 1996).

70. *Id.* at 18. The nine risk categories are: credit risk, interest rate risk, liquidity risk, price risk, foreign exchange risk, transaction risk, compliance risk, strategic risk and reputation risk.

71. Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies, Fed. Res. SR Letter 95-51 (Nov. 14, 1995), http://www.federalreserve.gov/boarddocs/SRLETTERS/1995/SR9551.htm (last visited Mar. 3, 2001).

72. *State/Federal Supervisory Protocol and Nationwide Supervisory Agreement* [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 46-145 (Fed. Res. SR Letter 96-33, Nov. 22, 1996), *available at* http://www.federalreserve.gov/boarddocs/SRLETTERS/1996/SR9633.htm (last visited Mar. 3, 2001).

73. *Risk-Focused Framework for Supervision of Large Complex Institutions,* [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 37-748C (Fed. Res. SR Letter 97-24, Oct. 27, 1997), *available at* http://www.federalreserve.gov/boarddocs/SRLETTERS/1997/SR9724. htm (last visited Mar. 3, 2001).

74. Risk-Focused Framework for the Supervision of Community Banks [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 37-748 (Fed. Res. SR Letter 97-25, Oct. 1, 1997), *available at* http://www.federalreserve.gov/boarddocs/SRLETTERS/1997/SR9725.htm (last visited Mar. 3, 2001).

have become focused on risk assessment, monitoring and control. Two issuances by the preeminent international bank regulatory body, the Basel Committee on Banking Supervision (referred to in this section as the "Basel Committee" or "Committee"),[75] are particularly useful in charting the development of risk-based supervisory concepts as applied to electronic banking and information technology.

In March 1998, the Basel Committee issued a document entitled "Risk Management for Electronic Banking and Electronic Money Activities."[76] In this document, one of the Committee's first attempts to deal on a broad basis with the risks attendant to electronic banking, the Committee stated that its purpose was to "provide considerations for supervisory authorities and banking organizations as they develop methods for identifying, assessing, managing and controlling the risks associated with electronic banking and electronic money."[77] The Committee noted that because of rapid changes in information technology, no list of risks involved in electronic banking activities can be exhaustive; however, the specific risks faced by banks engaged in electronic banking activities could, in the Committee's view, be grouped according to the risk categories that the Committee had established in its earlier issuances on the subject of risk management.[78] The Committee concluded that, although some

75. The Basel Committee On Banking Supervision is a committee of bank supervisory authorities that was established in 1974 by the central bank governors of the Group of Ten countries. The Committee comprises senior representatives of bank supervisory authorities and central banks from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Sweden, Switzerland, the United Kingdom and the United States. It usually meets at the Bank for International Settlements (BIS) in Basel, Switzerland, and the BIS provides the permanent Secretariat for the Committee. The Committee has had a significant impact on bank supervisory and examination principles among the banking authorities of its member nations, the most notable being its widely followed risk-based capital framework.

76. BASEL COMMITTEE ON BANKING SUPERVISION, *supra* note 66, at 1.

77. *Id.*

78. *Id.* at 4. In its "Core Principles for Effective Banking Supervision," issued in September 1997, the Basel Committee identified eight risk categories that form the basis of a risk-based supervisory system: credit risk, country and transfer risk, market risk, interest rate risk, liquidity risk, operational risk, legal risk and reputational risk. The U.S. federal banking regulators largely have adopted these risk categories, with some modifications, in the risk-based supervisory approach that they have implemented. *See supra* note 87 and accompanying text.

specific problems can cut across all risk categories, at that stage in the evolution of electronic banking, operational risk, reputational risk and legal risk may be the most important risk categories that banks must face.[79]

---

79. *See supra* note 69, at 5. The Committee described "operational risk" as that arising from the bank's potential for loss due to significant deficiencies in system reliability or integrity. This risk can include security concerns, as banks may be subject to external or internal attacks on their systems or products; inadequately designed or implemented electronic banking and electronic money systems; and customer misuse. *Id.*

"Reputational risk" was defined as the risk of significant negative public opinion that results in a critical loss of funding or customers. Reputational risk may involve actions that create a lasting negative public image of overall bank operations, such that the bank's ability to establish and maintain customer relationships is significantly impaired. Reputational risk may also arise if actions by the bank cause a major loss of public confidence in the bank's ability to perform functions critical to its continued operation. Reputational risk can arise in response to actions a bank itself takes or in response to actions of third parties. Increased reputational risk can directly contribute to heightened risk exposure, or problems, in other risk categories, particularly operational risk. *Id.* at 7. The Committee specifically pointed out that mistakes, malfeasance, and fraud by third parties may also expose a bank to reputational risk. Reputational risk can arise from significant problems with communications networks that impair customers' access to their funds or account information, particularly if there are no alternative means of account access. Indeed, substantial losses caused by mistakes of another institution offering the same, or similar, electronic banking products or services may cause a bank's customers to view its products or service with suspicion, even if the bank itself did not face the same problems. Reputational risk may also arise from targeted attacks on a bank. For example, a hacker penetrating a bank's web site may alter it to intentionally spread inaccurate information about the bank or its products. *Id.*

The Committee said that "legal risk" arises from violations of, or non-conformance with laws, rules, regulations, or prescribed practices, or when the legal rights and obligations of parties to a transaction are not well established. Given the relatively new nature of many retail electronic banking activities, rights and obligations of parties to such transactions are, in some cases, uncertain. For example, the application of some consumer protection rules to electronic banking activities in some countries may not be clear. In addition, legal risk may arise from uncertainty about the validity of some agreements entered into via electronic media. *Id.* at 8. The Committee also warned that banks choosing to enhance customer service by linking their Internet sites to other sites also can face legal risks. A hacker may use the linked site to defraud a bank customer, and the bank could face litigation from the customer. *Id.*

Finally, the Committee noted that as electronic commerce expands, banks may seek to play a role in electronic authentication systems, such as those using digital certificates. The role of a certification authority may expose a bank to legal risk. For example, a bank acting as a certification authority may be liable for financial losses incurred by parties relying on the certificate. In addition, legal risk could arise if banks participate in new authentication systems and rights and obligations are not clearly specified in contractual agreements. *Id.* A digital certificate issued by a certification authority is intended to ensure that a given digital signature is in fact generated by a given signer. A bank that undertakes to act as a

Although in its 1998 document the Basel Committee demonstrated a reasonably good grasp of the issues and risks presented by the industry's increasing involvement in electronic banking, the breadth and sophistication of the Committee's understanding and competence grew markedly in the two years following release of that paper. In particular, the Committee established an Electronic Banking Group ("EBG"), a subset of the Committee (presently chaired by the U.S. Comptroller of the Currency) that focuses entirely on electronic banking issues. The EBG issued a "White Paper" in October of 2000 titled "Electronic Banking Risk Management Issues for Bank Supervisors."[80] This paper extends the discussion begun in the 1998 document and highlights both the rapid growth of electronic banking in the two years since that paper was prepared. More importantly, the 2000 document evidences a much deeper understanding of the extent to which the growth of electronic banking has implications for a greater range of risks than had been presented in the 1998 paper.[81]

---

certification authority could be considered to be providing services to clients similar to those associated with providing an account access device or acting as a notary public. A digital signature is a string of data appended to an electronic message that is intended to identify uniquely the sender to the recipient. *See infra* notes 175-179 and accompanying text. At present, most digital signatures are generated using a cryptographic algorithm in which the sender uses one mathematical function to create the signature and the receiver uses a different, but related mathematical function to verify the signature. Digital signatures also typically provide a mechanism for verifying the integrity of the message. BASEL COMMITTEE ON BANKING SUPERVISION, *supra* note 66, at 8 n.7.

80. *See* ELECTRONIC BANKING RISK MANAGEMENT ISSUES FOR BANK SUPERVISORS, BASEL COMMITTEE ON BANKING SUPERVISION, http://www.bis.org/publ/bcbs76.pdf (Oct. 2000). This is one of a series of White Papers prepared by the Committee and released as part of a document titled "Electronic Banking Group Initiatives and White Papers." Please note that Committee publications are is not entirely consistent in references to the Committee's name ("for Banking" versus "on Banking") or the spelling of the Committee's home city, opting for the German-derived "Basel" in some instances and the French-derived "Basel" in others. *Id.*

81. *Id.* Section IV of the 2000 White Paper. Section IV contains an excellent discussion of the EBG's more current assessment of risks of electronic banking. Most significantly, the 2000 White Paper improves on the 1998 White Paper by adding a discussion of strategic and business risks, and by providing a much more detailed discussion of the various categories of operational risks. The discussion of operational risks covers more specifically the risks inherent in technology, infrastructure, security, data integrity, system availability, internal controls/audit, and outsourcing. *Id.*

5. Guidance from the U.S. Regulatory Community

The U.S. bank regulatory agencies are active participants in the Basel Committee, and much of the analysis and guidance contained in the Basel Committee issuances discussed above also can be found in releases from the U.S. regulators. Indeed, the U.S. regulators, both individually and jointly through the Federal Financial Institutions Examination Council ("FFIEC"), have been aggressive in disseminating to their institutions handbooks, bulletins and other forms of guidance dealing with various aspects of electronic banking, information technology and the risks inherent in those endeavors.

In 1996, the FFIEC issued its "Information Systems (IS) Examination Handbook."[82] At that point, the emphasis was on risk-based examinations of the internal processes and procedures employed by financial institutions in their handling and use of data and information. It was principally an inward-looking examination program, focusing on what the FFIEC called "transaction risk [that is,]... risks...associated with service or product delivery and with providing support in... management processes."[83] In more recent issuances, the FFIEC began to deal more directly with shared-risk issues. For example, in July 1998 the FFIEC issued its "Guidance on Electronic Financial Services and Consumer Compliance."[84] And in November of 2000, the FFIEC got to the heart of the matter when it published "Risk Management of Outsourced Technology Services." [85]

In addition to their coordinated efforts under the FFIEC umbrella, each of the bank regulatory agencies has issued its own analysis of and guidelines regarding electronic banking and technology risks. The OCC has been the most active in this regard. For example, the OCC published its own "Internet Banking

82. FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, 1996 INFORMATION SYSTEMS EXAMINATION HANDBOOK (Sept. 19, 1996) [hereinafter referred to as the IS HANDBOOK].

83. *Id.* at 2-1.

84. FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, GUIDANCE ON ELECTRONIC FINANCIAL SERVICES AND CONSUMER COMPLIANCE (July 15, 1998).

85. FEDERAL FIN. INST. EXAMINATION COUNCIL, RISK MGMT. OF OUTSOURCED TECH. SERVICES (Nov. 28, 2000).

Handbook" in October 1999.[86] Other examples include two 1998 issuances on "Technology Risk Management;"[87] issuances in 1999 on "Infrastructure Threats from Cyber-Terrorists"[88] and "Certification Authority Systems;"[89] and in 2000 on "Infrastructure Threats – Intrusion Risks,"[90] "Protecting Internet Addresses of National Banks,"[91] and "Third-Party Risk."[92]

The OCC has recognized implicitly that banks, through the increased use of technology-based delivery channels, have moved increasingly into a shared-risk environment. This can be seen, for example, in the OCC's August 24, 1998 release titled " Technology Risk Management: PC Banking."[93] In this document, the OCC provides guidance to banks on identifying, measuring, monitoring and controlling risks that arise from giving customers the option to use personal computers to effect banking transactions. In its summary of key points, the OCC notes:

> PC banking can increase the level of direct interaction between a bank's customers and its internal networks and technology systems and can expand the connections between public networks, such as the Internet, and the bank's internal systems. Without proper internal controls, these

86. OCC HANDBOOK ON INTERNET BANKING (October 1999), *available at* http://www.occ.treas.gov/handbook/intbank.pdf (last visited Mar. 4, 2001).

87. *Technology Risk Management,* [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 60-559 (OCC Bulletin 98-3, Feb. 4, 1998) [hereinafter OCC Bulletin 98-3]; *Technology Risk Management – PC Banking*, [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 60-731 (OCC Bulletin 98-38, Aug. 4, 1998) [hereinafter OCC Bulletin 98-38].

88. *Infrastructure Risk from Cyber-Terrorists*, [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 60-635 (OCC Bulletin 99-9, Mar. 5, 1999).

89. *Certification Authority Systems*, [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 60-732 (OCC Bulletin 99-20, May 4, 1999).

90. *Infrastructure Threats – Intrusion Risks*, [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 60-638 (OCC Bulletin 2000-14, May 15, 2000).

91. *Protecting Internet Addresses of National Banks*, [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 60-639 (OCC Alert 2000-9, July 19, 2000).

92. *Third Party Risk Analysis*, [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 35-521 (OCC Advisory Letter, Aug. 29, 2000). All of the OCC materials referenced in footnotes 86 through 91 may be accessed through links found on the OCC's "Internet Banking" web page, http://www.occ.treas.gov/netbank/ebguide.htm. (last visited Mar. 4, 2001).

93. OCC Bulletin 98-3, *supra* note 87, at 69,309.

situations may create significant security concerns.

In many cases, PC banking increases a bank's reliance on service providers and software vendors. Reliance on these third parties requires bank management to design appropriate risk controls for these relationships. [94]

The OCC has reported that although technology oriented bank systems are susceptible to the nine risks enumerated by the OCC, the greatest risks come from "strategic, reputation and compliance risk."[95]

Although the OCC has perhaps been the most active of the agencies in issuing guidance on technology issues, the other banking agencies early on also focused on shared--risk issues. For example, in the Information Technology section of its Regulatory Handbook, adopted in October 1997, the Office of Thrift Supervision ("OTS") advised its examination staff:

---

94. *Id.*

95. *Id.* at 69,114. The OCC found that *transaction risk*, the risk to earnings or capital arising from problems with the service or product delivery, can result "from deficiencies in system design, implementation, or ongoing maintenance of systems of equipment" and can increase when banks merge, when banks hire outside contractors to design systems, when banks use "vendors to perform core bank functions," or when banks fail to establish adequate security measures, contingency plans, testing and auditing standards. *Id.* at 69,115. The OCC found that *strategic risk*, the risk to earnings or capital arising from adverse business decisions or improper implementation of those decisions, can arise "when management does not adequately plan for, manage, and monitor the performance of technology-related products, services, processes, and delivery channels," or "if management fails to understand, support, or use a technology that is essential for the bank to compete or if it depends on a technology that is not reliable." *Id.* at 69,116. The OCC found that *reputation risk*, the risk to earnings or capital arising from negative public opinion, may arise from "flawed security systems that significantly compromise customer privacy; inadequate contingency and business resumption plans that affect a bank's ability to maintain or resume operations and to provide customer services following system failures, fraud that fundamentally undermines public trust and large-scale litigation that exposes a bank to significant liability." *Id.* The OCC found that *compliance risk*, the risk to earnings or capital arising from violations of or non-conformance with laws, rules regulations, prescribed practices, or ethical standards, may arise "when a bank does not have systems in place to ensure compliance with mandatory reporting statutes." *Id.* "As banks move increasingly from paper to electronic-based transactions and information exchanges, they need to consider how laws designed for paper-based transactions apply to electronic-based transaction and information exchanges." *Id.*

> With the increased focus of institutions on the use of electronic channels to perform their daily operations and offer new products and services, safety and soundness examiners play a more important role in evaluating an institution's risks in the use of information technology. Whether the institution's deployment of technology is limited to the staff's use of stand-alone personal computers (PCs) or includes more sophisticated applications such as telephone or PC banking programs for customers, the rapid pace of change in the electronic networked environment calls for a risk-based approach to examinations of institutions....
>
> Regardless of the level of sophistication, risks are inherent in all electronic capabilities. Threats can come from both internal and external sources. Outside hackers, disgruntled employees, and inadvertent errors can adversely affect reliability. For instance, an information-only World Wide Web site used for advertising purposes may be inappropriately altered by unauthorized parties. Electronic mail containing confidential or proprietary information may be distributed in error. Networked systems that are directly connected to an institution's main operations database might be accessed by unauthorized parties, revealing sensitive data.[96]

Similarly, the Federal Reserve in 1996, in reaction to the increasing use of computer technology, sought to benchmark sound information security policies and practices, and issued on December 4, 1997 Supervisory Release 97-32 (SUP), "Sound Practices Guidelines for Information Security for Networks."[97] At

96. OTS REGULATORY HANDBOOK 341.1 (Oct. 1997).

97. *Information Security For Networks – Sound Practices Guidance,* [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 60-631 (Fed. Res. Bull. 97-32, Dec. 4, 1997).

about the same time, the FDIC on December 18, 1997 issued Financial Institution Letter 131-97, transmitting a paper entitled "Security Risks Associated with the Internet."[98] In the years following these seminal pronouncements, all of the agencies have continued, jointly and individually to issue further guidance on dealing with technology-driven risks.[99]

One area that calls for the particular attention of the regulatory agencies is technology outsourcing. Because of the increasing reliance by institutions on third-party service providers to support their technology initiatives, the agencies through the FFIEC issued a guidance document on November 28, 2000 entitled "Risk Management of Outsourced Technology Services."[100] The FFIEC notes that the use of third-party service providers can help financial institutions manage costs, obtain necessary expertise, expand customer product offerings, and improve services, but also can introduce an additional set of risks for the institution. This document provides risk-management guidance in the due diligence process used in selecting a service provider, in addressing contractual issues, and in conducting the oversight and monitoring of the service provider during the term of the relationship.

Finally, to underscore the growing attention being paid to shared-risk issues by the regulators, the interagency Suspicious Activity Report ("SAR") was amended in June 2000 to address technology-related issues. Financial institutions are required to file an SAR when encountering a known or suspected violation of law or a suspicious transaction relating to a money laundering activity or violation of the Bank Secrecy Act. The SAR procedures now include "Computer Intrusion" as a type of reportable "Suspicious Activity Information."[101] "Computer Intrusion" is defined in the instructions to the SAR form as

[G]aining access to a computer system of a financial

98. *Information Security System Risk – Internet*, [Current Binder] Fed. Banking Rep. (CCH) ¶ 60-634 (FIL 131-97, Dec. 18, 1997).

99. A list of recent significant technology-related releases by the Basel Committee, FFIEC, and the regulatory agencies is included as the Appendix to this article.

100. *See supra* note 54.

101. SUSPICIOUS ACTIVITY REPORT (SAR) FORM, [Current Binder] Fed. Banking Rep. (CCH) ¶ 51-987 (SAR Bull., June 19, 2000).

institution to:

> a. Remove, steal, procure or otherwise affect funds of the institution or the institution's customers;
> b. Remove, steal, procure or otherwise affect critical information of the institution including customer account information; or
> c. Damage, disable or otherwise affect critical systems of the institution.
>
> For purposes of this reporting requirement, computer intrusion does not mean attempted intrusions of websites or other non-critical information systems of the institution that provide no access to institution or customer financial or other critical information.[102]

III. BANK SECURITY IN AN INFORMATION AGE

As banking becomes more complicated, bank security becomes more complicated. Regulators are holding bank directors and executives responsible for understanding and controlling their banks' security infrastructure.[103] Yet security is never an absolute: as long as a valuable prize is accessible to any person, it may become accessible to the wrong people. The history of security is the story of a constant struggle – featuring increasingly advanced plans, methods and technologies – between the people holding treasure and those wishing to take the treasure away. Each group gains an advantage and the other reacts to the new rules of the game. Modern day Willie Suttons will continue to attack financial institutions with new and creative schemes, while management and security professionals must resist and react. Furthermore, current bank security must be concerned not only with protecting access to

---

102. *Id.*

103. Federal bank regulators clearly direct bank management to specifically oversee information security efforts. OCC Bulletin 98-3, *supra* note 87; OCC Bulletin 98-38, *supra* note 87; *Security Monitoring of Computer Networks*, [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 60-640 (FIL 67-2000, Oct. 3, 2000).

cash by thieves, but also with maintaining customer accessibility and public confidence.[104]

These concerns broaden an organization's security mandate so that the organization must be proactive, flexible and constantly vigilant. Keeping people out of a bank is an easier task that assuring that everyone can come into the bank but that only those with permission may take money out. Today's banker must worry about terrorists, recreational hackers, and power disruptions as much as he worries about bank robbers.

Given these pressing demands, a bank could spend its entire budget on security measures and still never attain complete and certain security. Somehow, financial institutions must meet the practical and regulatory requirements for securing their electronic infrastructures without "breaking the bank." Financial services regulators provide detailed guidance and recommendations on security actions that regulated institutions should follow.[105] These guidelines are based on fundamental security practices applicable to any complex organization. Therefore, to understand the basis of regulatory and legal responsibilities for electronic information security, and to find efficient and effective

---

104. Banks risk business losses if the public does not perceive security in the banks' systems. For example, in a recent poll of American adults, those with Internet access most often cited security and privacy reasons as a reason for not banking online. Edward Morawski, *Industries, Poll: Net Currency*, RED HERRING, Jan. 16, 2001, *available at* www.redherring.com/industries/2001/0111/ind-mag-90-banking 011101.html (last visited Feb. 20, 2001). Bank regulators find reputation risk exposure in customer access issues. OCC Bull. 98-3, *supra* note 87.

> Reputation risk exposure is present throughout the organization and is why banks have the responsibility to exercise an abundance of caution in dealing with its customers and community.... Reputation risk arises whenever technology-based banking products, services, delivery channels, or processes may generate adverse public opinion such that it seriously affects a bank's earnings or impairs capital.... Adverse public opinion may create a lasting, negative public image of overall bank operations and thus impair a bank's ability to establish and maintain customer and business relationships.

Id. "In a general way, [bank] supervisory authorities are asked to give a certain nebulously defined protection to the public and the shareholders of banks, and in the event of failure or liquidation of the bank, specifically to its depositors." ROSS M. ROBERTSON, THE COMPTROLLER AND BANK SUPERVISION, 164-165 (1968).

105. *See* attached Appendix (citing regulatory releases from OCC, FDIC, Federal Reserve and OTS).

security practices, financial service executives and their counsel should become familiar with the security guidelines used as standards for government and industry. Bank management can learn the standard of care required for protecting its information systems by learning and enacting basic information security principles. To this end, the final section of this paper analyzes several well-established models for securing an organization built on networked electronic information, then proposes specific methods for pursuing cost-effective information security.

A. Information Security Methods and Theory

A simple and effective method of learning information security concepts is to review relevant theoretical models. The authors have chosen to examine the following three information security models: (1) a bank regulatory model evinced by the FDIC Issues Paper on Information System Security Issues[106] and the OCC's Technology Risk Management Guidance for Bankers and Examiners,[107] (2) the Generally Accepted Principles and Practices for Securing Information Technology Systems from the National Institute of Standards and Technology (NIST),[108] and (3) the Information Assurance Technology Framework (IATF) from the National Security Agency and private industry groups.[109] The following paragraphs describe similarities and differences in these three models and discuss how the information security models may apply to financial services companies.

Financial service regulators are charged with guiding banks in managing and controlling risk. As demonstrated above, many of these regulators have adopted a risk-based review of financial

106. *Risk Assessment Tools and Practices for Information System Security*, [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 60-636 (FIL-68-99, July 7, 1999).

107. OCC Bull. 98-38, *supra* note 87.

108. MARIANNE SWANSON & BARBARA GUTTMAN, GENERALLY ACCEPTED PRINCIPLES AND PRACTICES FOR SECURING INFORMATION TECHNOLOGY SYSTEMS (1996), *at* http://csrc.nist.gov/publications/nistpubs (last visited Mar. 4, 2001).

109. NATIONAL SECURITY AGENCY AND INFORMATION ASSURANCE SOLUTIONS, INFORMATION ASSURANCE TECHNOLOGY FRAMEWORK, RELEASE *3.0* (Oct. 2000), *at* https://www.iatf.net/login/framework_docs (last visited Mar. 4, 2001) (application for free password required) [hereinafter IATF] (describing the information security Defense-in-Depth Strategy used by the U.S. Department of Defense). *Id.*

institutions, and the analysis of risk is followed by recommended strategies for risk reduction;[110] OCC 98-3 is a representative example of these recommended strategies. In this guidance document, the OCC takes broad strokes to paint an outline of policies, plans and practices that may lead to reduction of security risk. Knowing that banks of varying sizes and in varying stages of technology development also have varying technology security needs,[111] the OCC only makes general recommendations salted with illustrative examples. The OCC does not provide safe harbors or detailed protection plans for its regulated entities.

After first defining the relevant risks involved with banks' growing dependence on technology, the OCC provides a "Technology-Related Risk Management Process."[112] To follow the OCC's recommended process, a bank must "(1) *plan* for its use of technology, (2) decide how it will *implement* the technology, and (3) *measure and monitor risk-taking.*"[113] After a detailed discussion of recommended strategies for strategic planning[114] and project management controls,[115] the OCC specifically speaks to the importance of security matters.[116] The regulatory guidance offers few specifics on information security beyond recommending fraud prevention, management involvement and regular audits.[117] The

110. *See, e.g.,* OCC Bull. 98-38, *supra* note 87; *Information Security For Networks – Sound Practices Guidance,* [Current Binder] Fed. Banking L. Rep. (CCH) ¶ 60-631 (Fed. Res. Bull. 97-32, Dec. 4, 1997).

111. *See* OCC Bull 98-3, *supra* note 93, at 6. "The process will be more complex for larger institutions, particularly for those with major technology-related initiatives." *Id.*

112. *Id.*

113. *Id.* The OCC warns that in reviewing banks it will "look to see that an effective planning process exists, that technology is implemented properly with appropriate controls, and that measurement and monitoring efforts effectively identify ways to manage risk exposure." *Id.*

114. *Id.* at 6-9.

115. *Id.* at 9-10.

116. *Id.* at 10. "Bank information system security controls are particularly important." *Id.* at 10.

117. *Id.* The entire information security statement in OCC 98-3 reads as follows:

> Security measures should be clearly defined with measurable performance standards. Responsible personnel should be assigned to ensure a comprehensive security program. Bank management should take necessary steps to protect mission-critical systems from unauthorized intrusions. Systems should be safeguarded, to

document then addresses other security-related topics in an equally cursory manner, including brief statements on policies and procedures, employee experience and training, measuring and testing products and performance, contingency planning and outsourcing.[118]

The FDIC issued a Financial Institution Letter discussing information security in financial institutions.[119] While the body of the letter provided general guidance to financial institution boards of directors, including an outline of a proactive "Prevention, Detection, Response" information security program,[120] the FDIC attached an appendix addressing certain of the most important tools and methods used to test an organization's information protection regime.[121] The FDIC letter analyzes risk[122] and reviews potential threats,[123] but like the OCC pronouncements, it does not

---

> the extent possible, against risks associated with fraud, negligence, and physical destruction of bank property. Control points should include facilities, personnel, policies and procedures, network controls, system controls and vendors. For example, security access restrictions, background checks on employees, separation of duties, and audit trails are important precautions to protect system security within the bank and with vendors. As technologies and systems change or mature, security controls may need to change periodically as well.

Id.

118. *Id.* at 10-14. For example, in the important security and risk-reduction field of "Contingency Planning and Business Continuity" the OCC declares that "The risk of equipment failure and human error is possible in all systems," and then describes various types of potential system failure. While OCC 98-3 discusses "public relations and outreach" as a part of business continuity planning, this document does not provide guidance on the specific content of an acceptable contingency plan. *Id.*

119. FDIC FIN. INST. LETTER, *supra* note 54.

120. *Id.* at 1-2.

121. *Id.* at 6-11.

122. *Id.* at 3. The letter examines performance of internal security risk assessments (including outsourcing such assessments) and assessing information security products. The FDIC recommends "identifying mission-critical information systems,... assessing the importance and sensitivity of information,... the likelihood of outside break-ins (e.g., by hackers),...insider misuse of information,...assessing the risks posed by electronic connections with business partners [and] determining legal implications and contingent liability concerns associated with any of the above." FDIC FIN. INST. LETTER, *supra* note 54, at 3.

123. "Serious hackers, interested computer novices, dishonest vendors or competitors, disgruntled current or former employees, organized crime, or even agents of espionage pose a potential threat to an institution's computer security." *Id.* The letter also warns of "social engineering... denial of service" system failure attacks, Internet protocol spoofing, and viruses. *Id.* at 3-4.

provide comprehensive or detailed advice on what actions banks should take to protect digital information. The closest the FDIC comes to specific advice on security methodologies is its appendix discussing host-based and network-based vulnerability assessment tools,[124] penetration analysis,[125] intrusion detection systems,[126] and computer incident response.[127] While the FDIC does not officially endorse these security practices, financial service institutions would be well served to consider the FDIC's discussion as a note of warning to consider implementing some or all of these tools as protection for an information infrastructure.

For a bank manager to understand what these regulators require, and to implement these broad regulatory directives, its management should study the more detailed information security

---

124. *Id.* at 5-6. "Both host- and network-based products offer valuable features, and the risk assessment process should help an institution determine which is best for its needs. Information systems personnel should understand the types of tools available, how they operate, where they are located, and the output generated from the tools." *Id.* at 5.

125. *Id.* at 6. Penetration analysis "can apply to any institution with a network, but becomes more important if system access is allowed via an external connection such as the Internet." The FDIC also warns that a penetration analysis "itself can introduce new risks to an institution," and recommends in-depth analysis of the reputation of a consultant hired to do such testing (including review of liability insurance, security clearance and confidentiality agreements), recommends informing key individuals prior to a penetration test, and recommends that some systems may be too critical to expose to such testing at all. *Id.*

126. *Id.* Intrusion detection systems "act as a burglar alarm, reporting potential intrusions to appropriate personnel. By analyzing the information generated by the systems being guarded, [intrusion detection systems] help determine if necessary safeguards are in place and are protecting the system as intended. . . [and] they can be configured to automatically respond to intrusions." *Id.* The FDIC goes on to discuss the relative merits of intrusion detection systems including software sniffer agents on networks and host-based audit products, but does not endorse any one system for use in a financial institution. *Id.* at 6-7.

127. *Id.* at 9. The FDIC observes that current tools allow for real-time monitoring of system intrusions and therefore automatic and immediate response.

> When determining an appropriate response, a distinction should be made between incidents in which actual changes to a system are suspected (e.g. changing audit logs) versus incidents in which system misuse is suspected (e.g. unauthorized system access). Attempts to actually change the system or data may warrant notifying a security officer, who could reconfigure the identified weakness and/or communication paths. An appropriate response to system misuse may include automatic log-off, warning messages, or notifying the appropriate personnel.

Id. at 9.

models written for security professionals in government and across all industries. For example, the National Institute of Standards and Technology[128] has issued a relevant document titled "Generally Accepted Principles and Practices for Securing Information Technology Systems."[129] Like the financial service regulators, the NIST provides some broad principles in this document that "address computer security from a very high-level viewpoint," and are to be used "when developing computer security programs and policy and when creating new systems, practices or policies."[130] The NIST document describes eight general principles for computer security:

> 1. computer security supports the mission of the organization;
> 2. computer security is an integral element of sound management;
> 3. computer security should be cost effective;
> 4. system owners have security responsibilities outside own organizations;
> 5. computer security responsibilities and accountability should be made explicit;
> 6. computer security requires a comprehensive and integrated approach;
> 7. computer security should be periodically reassessed; and
> 8. computer security is constrained by societal factors.[131]

Such overarching security platitudes, while valid, have limited use in planning information protection regimes.

---

128. The National Institute of Standards and Technology is a one hundred year old agency of the U.S. Department of Commerce's Technology Administration. NIST is charged with working with industry to develop and apply technology, measurements and standards. NIST sponsors the Malcolm Baldridge Quality Awards, the U.S. Measurements and Standards Laboratories, and an Advanced Technology Program. *See* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *at* http://www.nist.gov/public_affairs/general2.htm (last visited Mar. 4, 2001).

129. *See* SWANSON & GUTTMAN, *supra* note 108.

130. *Id.* at 1. "Principles are expressed at a high level, encompassing broad areas, e.g., accountability, cost effectiveness, and integration." *Id.*

131. *Id.* at iii.

However, the NIST security recommendations do not leave the interested student hanging in the ether. NIST provides very specific current practices to "guide organizations on the types of controls, objectives and procedures that comprise an effective IT security program."[132] The security practices identified by NIST range from creating a protection policy to administration and staffing, from physical and environmental security to contingency planning.[133] While space does not permit a complete analysis of the NIST security practices, two important security topics are highlighted here.

First, the NIST document includes a helpful short discussion of information technology life cycle planning.[134] NIST recommends that organizations develop a security plan to ensure that security is considered throughout the entire life cycle of an information technology system, including an assessment of the sensitivity of information to be processed on the system.[135] As an organization acquires, designs or programs the system, security requirements should be written into the initial specifications. The organization should be monitoring for threats that may arise in the development phase like "Trojan horses,[136] incorrect code, poorly

132. Swanson and Guttman state that,

> The practices show what should be done to enhance or measure an existing computer security program or to aid in the development of a new program. The practices provide a common ground for determining the security of an organization and build confidence when conducting multi-organizational business... Organizations should use the practices as a starting point in order to develop additional practices based on their own organizational and system requirements.

Id. at 1-2.

133. *Id.* at 11-54. The NIST authors discuss security practices in the following categories: Policy, Program Management, Risk Management, Technology Life Cycle Planning, Personnel/User Issues, Preparing for Contingencies and Disasters, Computer Security Incident Handling, Awareness and Training, Security Considerations in Computer Support and Operations, Physical and Environmental Security, Identification and Authentication, Logical Access Control, Audit Trails, and Cryptography. *Id.* at iv.

134. *Id.* at 22-26.

135. *Id.* at 22.

136. This term is well defined in Ford and Baum's discussion of planting:

functioning development tools, manipulation of code, and malicious insiders."[137] During the implementation phase, when a system is installed and tested, NIST recommends initial system security testing[138] and formal accreditation.[139] The next technology life cycle phase is the operation/maintenance phase which should include standard security administration activities,[140] operational assurance and continual audits.[141] In the final phase of an information technology system life cycle (which NIST calls "disposal phase"), the organization disposes of information, hardware and software. NIST warns that in this phase the organization must follow legal records retention rules and must archive or move encrypted information. The organization should

---

> Usually as a follow-up to a system penetration or authorization violation attack, an intruder leaves behind a planted capability to perpetrate or aid future attacks. Variations include *Trojan Horse*: Software which outwardly has a legitimate purpose but which, when executed, compromises the security of the user. An example of a Trojan horse is a screen-saver that, while creating a pretty screen image, surreptitiously scans a PC's memory and disk files for character strings formatted as credit card numbers and sends all such strings to an external network address accessible by the attacker.

WARWICK & MICHAEL S. BAUM, SECURE ELECTRONIC COMMERCE: BUILDING THE INFRASTRUCTURE FOR DIGITAL SIGNATURES AND ENCRYPTION 96 (2nd ed., 2001).

137. SWANSON & GUTTMAN, *supra* note 108, at 22-23.

138. Experts note that:

> System security testing includes both the testing of the particular parts of the system that have been developed or acquired and the testing of the entire system. Security management, physical facilities, personnel, procedures, the use of commercial or in-house services (such as networking services), and contingency planning are examples of areas that affect the security of the entire system, but may have been specified outside of the development or acquisition cycle.

Id. at 23-24.

139. *Id.*

140. "Performing backups, holding training classes, managing cryptographic keys, keeping up with user administration and access privileges, and updating security software are some examples." *Id.* at 24.

141. NIST describes the standard security audit techniques as Automated Tools (including "(1) active tools, which find vulnerabilities by trying to exploit them, and (2) passive tests, which only examine the system and infer the existence of problems from the state of the system"), Internal Controls Audit, Security Checklists (or "baselines"), and Penetration Testing (attempting a system break-in, preferably conducted with the consent and knowledge of the system manager). *Id.* at 25.

also consider long-term storage of cryptographic keys.[142] Media should be sanitized before the organization disposes of it.[143] Clearly, security risks abound in all phases of a system's life cycle, and financial services companies will not meet their regulatory dictates without choosing practices to address each of the threats described above.

As a second example of specific security practices, this paper describes NIST's treatment of user authentication for access to electronic systems. According to NIST, "Identification and Authentication" is a "technical measure that prevents unauthorized people (or unauthorized processes) from entering an [information technology] system."[144] User identification, "the means by which a user provides a claimed identity to the system," should include a unique identifier for every user, internal correlation of users to their actions within the system, and disabling of inactive users.[145]

The second part of assuring someone's identity online is

142. The organization must also remember to store the access methods for retrieving and using these keys. *Id.* at 26.

143. Swanson and Guttman point out that,

> The removal of information from a storage medium (such as hard disk or tape) is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by keyboard attack) and purging (rendering information unrecoverable against laboratory attack). There are three general methods of purging media: overwriting, deguassing (for magnetic media only) and destruction.

SWANSON & GUTTMAN, *supra* note 108, at 26.

144. *Id.* at 43.

> Identification and Authentication is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability .... Access control usually requires that the system be able to identify and differentiate among users. For example, access control is often based on *least privilege*, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an [information technology] system to specific individuals and, therefore, requires the system to identify users.

Id.

145. *Id.* at 43.

authentication. User authentication is the means to establish the validity of access to a system.[146] To operate a secure network, users should be required to authenticate their identities (usually with a single log-in to the system). An organization wishing to secure its network should secure transmission of this data over public or shared networks,[147] should make the display of authentication data as it is entered, and should limit the number of log-in attempts for any user ID.[148] If an organization has chosen to use passwords for authentication, it should change those passwords frequently, should carefully specify the characters used for the password,[149] and should train users on secure treatment of passwords. User training and administration are vital where an organization chooses more advanced forms of authentication like digital certificates or biometric devices.[150] The specificity provided by the NIST security practices helps clarify proper methods of securing information systems.

Another information security model is provided by the U.S. National Security Agency and its private industry partners in the Information Assurance Technical Framework (IAFT or

146. Swanson and Guttman point out that,

> There are three means of authenticating a user's identity *which can be used alone or in combination*: something the individual *knows* (a secret – e.g., a password, Personal Identification Number (PIN), or cryptographic key); something the individual *possesses* (a token – e.g., an ATM card or a smart card); and something the individual *is* (a biometric – e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint).

Id. at 44.

147. Experts have stated that,

> When authentication data, such as a password, is transmitted to an [information technology] system, it can be electronically monitored. This can happen on the network used to transmit the password or on the [information technology] system itself. Simple encryption of a password that will be used again does not solve this problem because encrypting the same password will create the same ciphertext; the ciphertext becomes the password.

Id.

148. SWANSON & GUTTMAN, *supra* note 108, at 44.

149. "Secure password attributes such as minimum length of six [characters], inclusion of special characters, not being in an online dictionary, and being unrelated to the user ID should be specified and required." *Id.* at 45.

150. *Id.*

Framework).[151] The IATF was written to provide "technical guidance for protecting United States (U.S.) Government and industry information and information infrastructures." "Information assurance relies on *the people, the operations, and the technology* to accomplish the mission/business and to manage the technology/information infrastructure."[152] The IATF is an intricately detailed document, first defining information infrastructure, describing the Defense-in-Depth information assurance strategy, and explaining the highly technical aspects of security engineering, technical countermeasures, network defense, perimeter defense and supporting infrastructure.[153] Any bank manager, security professional or attorney interested in understanding current regulatory and legal standards for information security can gain insight from the entire IATF document. The following paragraphs focus only on the Defense-in-Depth strategy highlighted there. The minutia of Public Key Infrastructure, Virtual Private Networks and Electronic Enclave Boundaries are important to protecting complex shared-risk information systems, but are beyond the scope of this paper.

The Framework is built around a U.S. Department of Defense led strategy initiative called Defense-in-Depth. "The underlying principles of this strategy are applicable to any information system or network, regardless of organization."[154] Defense-in-Depth is a layered security strategy built around the following aspects of an organization: 1) the training, awareness,

151. IATF, *supra* note 109.

152. *Id.* at iii. (Forward by Cynthia Frederick, IATF Technical Director). The IATF is intended for system security engineers, security customers, scientists and researchers, commercial product and service providers and standards bodies and consortia. *Id.* § 1.2.

153. *Id.* §§ 2.1.1-.4. The IATF not only describes the Defense-in-Depth Objectives, but also addresses: 1) An information system security engineering process including systems acquisition, risk management, technology life-cycle support and certification; 2) Technical security countermeasures including multi-level strategies, interoperability framework, and considerations for a public key infrastructure; 3) Defending the network, including availability of backbone networks, wireless network security, virtual private networks and secure voice communication; 4) Defending the enclave boundary, including firewalls, remote access, and malicious code protection; 5) Defending the computing environment and 6) Information assurance for the tactical environment. *Id.* §§ 1.1-9.11.

154. *Id.* § 1.4.

physical security, personnel security and system security administration of an organization's *people*; 2) the framework, security criteria, acquisition, risk assessment, certification and accreditation of an organization's *technology*; 3) and the assessments, monitoring, intrusion detection, warning, response and reconstitution of an organization's *operations*.[155] The strategy is built to protect information in complex organizational structures while allowing access to information. The framework document states:

> The dominant need of the user community is ready access to the information and information infrastructure needed to support their operational objectives. This requires the use of robust information processing technology and reliable connectivity. [Information assurance] enables these capabilities by providing organizations with the capacity to maintain adequate protection of their information.[156]

The technology aspect of Defense-in-Depth concentrates around four focus areas: (1) Defending the Computing Environment; (2) Defending the Enclave Boundary; (3) Defending the Network and Infrastructure; and (4) Supporting Infrastructures.[157]

An organization's computer users must be required to protect their internal servers and system applications, or Computing Environment. "This includes Identification and

---

155. *Id.*

> Of the three principal aspects of this strategy, the IATF focuses on technology and on providing overlapping layers of protection against cyber threats. By this approach, a successful attack against one layer or type of protection does not result in the compromise of the entire information infrastructure. Other policies, procedures, and frameworks are focused on addressing the people and operations aspects of a Defense-in-Depth strategy.

Id.

156. *Id.* § 2.1

157. IATF, *supra* note 109, §§ 2.1.1 –.4.

Authentication, access control, confidentiality, data integrity, and non-repudiation services for the variety of legacy and emerging applications within system high environments."[158] Defending the Enclave Boundary is the electronic version of the ageless strategy of perimeter defense. It means protecting an organization's information infrastructure from intrusion as the organization's private network connects to public or shared networks.[159] An organization is Defending the Network and Infrastructure Objectives when it protects information from unintentional disclosure or alteration.[160] "Supporting infrastructure components are needed to be able to detect and respond such as intrusion detection systems, audit, configuring the system, or collecting data needed for an investigation."[161] While the IATF concentrates on the technology aspects of information security and only skims the surface of the personnel and operational aspects, the Framework's detailed layering of security and strong cryptographic elements give insight into methods and practices for keeping financial institution information secure.

Each of the security models examined above provides guidance to bank management seeking to improve information security in a shared-risk system. By studying differences in the security models a manager can learn what each authoring body feels is most important in creating a security system. By studying

158. *Id.* at § 2.1.1. Objectives in Computing Environment security include ensuring the confidentiality and integrity of data, defending against unauthorized use of client and server, and ensuring adequate defenses against subversive acts of trusted people and systems. *Id.*

159. *Id.* at § 2.1.2. Objectives in keeping intruders out of an organization's network include enabling "dynamic throttling of services in response to changing threats," providing "a risk-managed means of selectively allowing essential information to flow across the enclave boundary," and providing strong authentication for access control. *Id.*

160. *Id.* at § 2.1.3. When defending network and infrastructure objectives, the organization should assure that all information is protected from disclosure to anyone gaining unauthorized access to the network, should protect user traffic from outside traffic flow analysis, and should "ensure protection mechanisms do not interfere with otherwise seamless operation with other authorized backbone and enclave networks." *Id.*

161. *Id.* at § 2.1.4. An organization assuring supporting infrastructure should "provide a cryptographic infrastructure that supports key, privilege, and certificate management and that enables positive identification of individuals using network services" and should "plan execution and reporting requirements for contingencies and reconstitution." *Id.*

similarities the manager can draw conclusions about choosing priorities for protection of an electronic banking network and the information it contains. The final section of this paper reviews some of these conclusions and their applicability to financial services organizations.

B. Allocating Resources for Information Protection

No organization can afford to throw money into a pit of unnecessary and inadequate security measures. Instead, all financial services organizations must find a way to meet the regulatory mandates and sensible business practices of strong information security by spending on the most effective protections.[162] The security models examined in the last section suggest that financial service companies should protect their information by developing careful security plans, by adopting authenticated, redundant infrastructure security, and by training people to value security.

Business security is a process, not a destination. As discussed above, no accessible assets are absolutely secure. A security team plans for defense, prepares technology to repel intrusions and avoid accidents, trains people to protect their own information, plans for disaster recovery, and remains constantly vigilant. Creating and following a well-considered and flexible security plan eases the process. Each of the security models reviewed in the previous section emphasizes planning as a primary element of strong information protection. When creating an information security plan, first map your organization's vulnerabilities. Where do you keep the crown jewels of your business information? Where is your network connected to the Internet? Where is it connected to your vendors' networks? Who

162. Simson Garfinkle comments regarding web security:

> Web security is not 'all or nothing' – security is a matter of degree. The more security measures you employ, the more you reduce your risk. Your goal should be to reduce risk as much as practical (and affordable), and then to take additional measures so that if there is a security incident, you will be able to recover quickly.

SIMSON GARFINKLE, WEB SECURITY AND COMMERCE (1997), at 24.

in your organization needs access to which information? Should your customers have access to the same information your employees see?

Next, choose strategies such as those described in the NIST practices or the IAFT for reducing these vulnerabilities.[163] Budget for the number and types of people and equipment needed to meet your design. Plan to provide more security where it will help the most, like perimeter choke points in your network, and less security in less vulnerable locations, like systems that are only accessed internally or basic office applications. Expect your security needs to change as your business changes and as technology progresses, so build flexibility into your plan. Online services and connectivity are continuing to grow, further complicating security, so plan for your security budget to grow, even if your business is not growing. Finally, plan for contingencies and disasters, so that your business can recover quickly should harm befall your information system.

A second lesson learned from the information security models is that a complex organization can benefit from an authenticated redundant information security architecture. This architecture is divided into a network layer, an application layer and system security. What technology should protect the communication of data from one network system to another (your "network layer")?[164] Safeguards for the network layer typically include tools and policies that promote authentication and integrity, confidentiality and access control.[165] What should protect the programs running on servers and personal computers,

163. For example, multi-layered security systems, public key infrastructure and other cryptographic protections, or penetration analysis and testing.

164. FORD & BAUM, *supra* note 136, at 144. The authors note:

> If an end system is connected directly to the Internet without [appropriate network security measures, any packet of data it receives potentially] may have been modified in transit, may not be from the source from which it appears to come, and may be part of a deliberate attack upon the system, [including penetration and denial-of-service attacks]. Also any packet sent [potentially] may not go where it is addressed, may get modified en route, and may be read by unknown people or systems.

Id.

165. *Id.* at 142-143.

like email, document management, or payment system software (your "application layer")?[166] Application-layer security can include authentication, access control, confidentiality, data integrity, and non-repudiation.[167]

Current security trends favor application-level security over network-level security,[168] but many organizations prefer a multi-tiered approach for more robust protection.[169] Multi-tiered protection may even be the most cost-effective solution.[170] The IATF document stated:

> Information infrastructures are complicated systems with multiple points of vulnerability. To address this, the IATF has adopted the use of multiple [information assurance] technology solutions within the fundamental principle of the *Defense-in-Depth* strategy, that is, using layers of [information assurance] technology solutions to establish an adequate [information assurance] posture. Thus, if one protection mechanism is successfully penetrated, others behind it offer additional protection. Adopting a strategy of layered protections does not imply that [information assurance] mechanisms are needed at every possible point in the network architecture. By implementing

166. *Id.* at 145.

> Some application[-layer] security services constitute an alternative to or a duplication of network[-layer] security services. [For example, application-layer encryption of messages between a Web browser and a Web server might achieve the same result as encryption of the traffic at the network (IP) layer]. However, many applications have special security requirements that just cannot be satisfied by network-layer security.

Id.

167. *Id.* at 146.

168. *Id.*

169. IATF, *supra* note 109, at § 1.4.1.

170. *Id.* "[A] layered strategy permits application of lower assurance solutions when appropriate, which may be lower in cost. This approach permits the judicious application of higher assurance solutions at critical areas (e.g., network boundaries)." *Id.*

> appropriate levels of protection in key areas, an effective set of safeguards can be tailored according to each organization's unique needs.[171]

What methods should be used to provide protection of a particular end system and its local environment (your "system security")?[172] The best-known system security attack involves exploitation of known weaknesses in software products.[173] System security safeguards include downloading software only from reliable sources, managing system passwords, and auditing system penetrations.[174]

In today's technical environment, authentication generally means more than use of a personal identification number (PIN) and password. Identification systems generally rely on something the user knows (PIN and password), something the user has ("tokens" like access cards or smart cards), or the identity of the user (biometrics, like fingerprint, handwriting, or voice image).[175] With the rapid commercialization of digital certificates (also called digital signatures),[176] public key cryptography is emerging as an important electronic tool for identification and authentication. Digital certificates improve any of the methods of identification. A brief description of public key cryptography may be helpful.[177]

---

171. *Id.* § 1.4.1.

172. "Historically, most system damage attributed to Internet-originated attacks could have been averted through adequate attention to system security." FORD & BAUM, *supra* note 136, at 147.

173. *See id.* at 315-403 (describing non-repudiation and digital certificate practices); MICHAEL S. BAUM & HENRY H. PERRITT, JR., ELECTRONIC CONTRACTING, PUBLISHING, AND EDI LAW 208-209 (1991) (discussing notary authentication); *Id.* at 197-207 (discussing security standards).

174. FORD & BAUM, *supra* note 136, at 146-47.

175. GARFINKLE, *supra* note 162, at 105-107. In addition, Garfinkle writes that "some companies are developing authentication systems based on Global positioning System[s]," authenticating a user by the user's location. *Id.* at 107.

176. This is not to be confused with the legal term of art for "electronic signature" as it is used in the Electronic Signatures in Global and National Commerce Act or other similar electronic commerce enabling statutes. Pub. L. No. 106-299, 114 Stat. 464, 465-473 (2000). These laws tend to broadly define an electronic signature as any recordable sign of assent that is independent of any specific technology solution like cryptographic digital certificates.

177. For a business-level discussion of digital certificates and public key cryptography *see* GARFINKLE, *supra* note 162, at 101-249; FORD & BAUM, *supra* note 132, at 181-285; IATF, *supra* note 109, § 8.1.

Digital certificates use cryptrographic algorythms called "keys" to authenticate identity. Each user of a digital certificate creates two keys: the user signs his message (e.g., email, document, or transaction order) with a *private key*, which the user keeps to himself, and can use to prove his identity; the user widely distributes his *public key*, which is applied by others to verify the user's certificate. As an example, a friend holds a copy of the user's public key. The friend sends the user message and asks him to certify it with his private key and send it back. When the friend receives the message back, she verifies the certification with the public key and then she knows that she is corresponding with the person that sent her the public key (presumably the user). To protect a private key, it can be encrypted and stored on a computer hard disk (this method is used by Netscape Navigator and the famous PGP program), it could be stored on a removable floppy disk or CD-ROM for greater security, or for even stronger protection it can be stored on a smart card.[178] A Public Key Infrastructure uses digital certificates to allow a trusted third party to vouch for the user's identity.[179] Financial service companies should be examining the use of digital certificates and a public key infrastructure to authenticate users and help secure basic financial transactions.

Just as Willie Sutton and John Dillinger reached the bank's money through its employees, the weakest information security link at many of today's banks are users of the bank's technology. Companies have learned the effectiveness of training employees to respect security and building policies and procedures to enhance security. If a company chooses to use digital certificates, it must create a digital certificate policy.[180] Financial services companies are required to post and follow customer privacy policies.[181] Banks should also be concerned with more basic security guidelines like those addressing use and regular changing of access passwords, document and email retention, Internet proxy servers, opening documents sent by email, and locked screen savers. Bank policies

178. GARFINKLE, *supra* note 162, at 108-110.
179. *Id.* at 112; FORD & BAUM, *supra* note 136, at 193-314.
180. *Digital Signature Guidelines*, 1996 A.B.A. SEC. OF SCI. AND TECH. 77.
181. *See supra* note 65.

should also limit network access of consultants and contractors, and limit the number of vendors with direct connections into bank systems.

IV. CONCLUSION

Banks have always attracted crooks and embezzlers because they held a great reward. Today's financial service companies have more threats to guard against and infinitely more complicated systems to secure. Digital money and other valuable digitized information call for a higher and more complex level of protection from financial services companies. Financial regulators have confirmed these new priorities. However, current bank managers can meet their protection obligations in the new environment by understanding current information security priorities, and can afford to meet their obligations if they plan well, implement effective authenticated, redundant systems, and prepare their people and policies to enhance information security. Banks may never stop a determined Willie Sutton, but by managing their security risks, banks can remain trusted holders of the public money.

V. APPENDIX

Significant Regulatory Releases on Bank Technology Issues (Available on Web Sites as Noted)

Basel Committee on Banking Supervision (http://www.bis.org)

October 2000:	Electronic Banking Group Initiatives and White Papers
March 1998:	Risk Management for Electronic Banking and Electronic Money Activities

Federal Financial Institutions Examination Council (http://www.ffiec.gov)

November 28, 2000:	Risk Management of Outsourced Technology Services
July 15, 1998:	Interagency Guidance on Electronic Financial Services and Consumer Compliance
September 1996	FFIEC Information Systems Examination Handbook

Office of the Comptroller of the Currency (http://www.occ.treas.gov)

January 2001:	Comptroller's Corporate Manual – The Internet and the National Bank Charter Handbook
January 17, 2001	Release 2001-4: Interagency Guidelines Establishing Standards For Safeguarding Customer Information (issued jointly with Federal Reserve, FDIC and OTS)

November 11, 2000	Advisory Letter 2000-12: Risk Management of Outsourcing Technology
July 7, 2000	Alert 2000-9: Protecting Internet Addresses of National Banks
May 15, 2000	OCC 2000-14: Infrastructure Threats – Intrusion Risks
February 11, 2000	Alert 2000-1: Internet Security: Distributed Denial of Service Attacks
October 1999	Comptroller's Handbook – Internet Banking
September 27, 1999	OCC 99-35: Interim Rule on Electronic Delivery of Disclosures
May 4, 1999	OCC 99-20: Certification Authority Systems
May 4, 1999	Advisory Letter 99-6: Guidance to National Banks on Web Site Privacy Statements
March 5, 1999	OCC 99-9: Infrastructure Threats from Cyber-Terrorists
August 24, 1998	OCC 98-38: Technology Risk Management: PC Banking
February 4, 1998	OCC 98-3: Technology Risk Management
November 19, 1997	Advisory Letter 97-9: Reporting Computer Related Crimes

Board of Governors of the Federal Reserve System (http://www.federalreserve.gov):

November 30, 2000	SR 00-17 (SPE): Guidance on the Risk Management of Outsourced Technology Services
February 29, 2000	SR 00-4 (SUP): Outsourcing of Information and Transaction Processing
February 29, 2000	SR 00-3 (SUP): Information Technology Examination Frequency
March 31, 1999	SR 99-8 (SUP): Uniform Rating System for Information Technology (with attached FFIEC January 20, 1999 release)
April 20, 1998	SR 98-9 (SUP): Assessment of Information Technology in the Risk-Focused Frameworks for the Supervision of Community Banks and Large Complex Banking Organizations
December 4, 1997	SR 97-32 (SUP): Sound Practices Guidance for Information Security for Networks
November 6, 1997	SR 97-28 (ENF): Guidance Concerning the Reporting of Computer-Related Crimes by Financial Institutions

Federal Deposit Insurance Corporation (http://www.fdic.gov)

November 9, 2000	FIL-77-2000: Bank Technology Bulletin
November 2, 2000	FIL-72-2000: Electronic Signatures in Global and National Commerce Act
October 3, 2000	FIL-67-2000: Security Monitoring of Computer Networks
September 21, 2000	FIL-63-2000: Online Banking
December 20, 1999	FIL-113-99: Financial Institution Web Site Privacy Survey
July 7, 1999	FIL-68-99: Risk Assessment Tools and Practices for Information System Security
August 17, 1998	FIL-86-98: Electronic Commerce and Consumer Privacy
July 16, 1998	FIL-79-98: Electronic Financial Services and Consumer Compliance
October 8, 1996	FIL-82-96: Risks Involving Client/Server Computer Systems
August 6, 1996	FIL-59-96: Stored Value Card and Other Electronic Payment Systems

Office of Thrift Supervision (http://www.ots.treas.gov)

June 10, 1999	CEO Memorandum 99-109: Transactional Web Sites
November 30, 1998	Final Rule on Electronic Operations
July 23, 1998	CEO Letter 90: Interagency Guidance on Electronic Financial Services and Consumer Compliance
December 23, 1997	CEO Letter 75: Guidance Concerning the Reporting of Computer-Related Crimes by Financial Institutions
October 15, 1997	OTS Thrift Activities Handbook, Section 341: Information Technology
June 23, 1997	Memorandum to Chief Executive Officers: Guidance to Thrifts on Retail On-line PC Banking
October 24, 1996	Memorandum to Chief Executive Officers: Risk Management of Client Server Systems